ESET SMART SECURITY 9

Uživatelská příručka

(platná pro produkty verze 9.0 a novější)

Microsoft® Windows® 10 / 8.1 / 8 / 7 / Vista / XP

Klikněte sem pro stažení nejnovější verze příručky

ENJOY SAFER TECHNOLOGY™

ESET **SMART SECURITY**

Technická podpora: www.eset.cz/podpora

REV. 7/1/2016

Obsah

Obsah

1. ESET Smart Security

ESET Smart Security představuje nový přístup k integrované počítačové bezpečnosti. Nejnovější verze skenovacího jádra ThreatSense® společně s Personálním firewallem a antispamovým modulem poskytují rychlou a přesnou ochranu počítače.Výsledkem je inteligentní systém, který neustále kontroluje veškeré dění na počítači na přítomnost škodlivého kódu.

ESET Smart Security je komplexní bezpečnostní řešení, které kombinuje maximální ochranu s minimálním dopadem na operační systém. Pokročilé technologie založené na umělé inteligenci jsou schopny proaktivně eliminovat viry, spyware, trojské koně, červy, adware, rootkity a další internetové hrozby, bez dopadu na výkon počítače nebo funkčnost operačního systému.

Funkce a přednosti

Přepracované uživatelské rozhraní	Grafické rozhraní ESET Smart Security bylo kompletně přepracováno. Nyní je čistější, přehlednější a intuitivnější. Nově jsme přidali také podporu pro jazyky se zápisem zprava doleva jako je Hebrejština a Arabština. Prostřednictvím online nápovědy získáte vždy nejrelevantnější informace k aktuálně zobrazenému dialogovému oknu a nápověda vám pomůže vyřešit váš problém.
Antivirus a antispyware	Proaktivně detekuje a léčí známé i neznámé viry, červy, trojské koně a rootkity. **Pokročilá heuristika** označí každý dosud neznámý malware, chrání vás před neznámými hrozbami a eliminuje je dříve, než mohou způsobit škodu. **Ochrana přístupu na web** a modul **Anti-Phishing** monitoruje komunikaci mezi internetovým prohlížečem a vzdálenými servery (včetně SSL). **Ochrana poštovních klientů** zajišťuje kontrolu komunikace pomocí POP3(S) a IMAP(S) protokolů.
Pravidelné aktualizace	Pravidelné aktualizace virové databáze a programových modulů zajistí maximální ochranu počítače.
ESET LiveGrid®	Můžete zkontrolovat reputaci běžících procesů a souborů přímo v ESET Smart Security vůči cloudové databázi.
Kontrola výměnných médií	Automaticky kontroluje všechny USB disky, paměťové karty a CD/DVD. Blokuje výměnná média podle typu, výrobce, velikosti a dalších atributů.
HIPS	Pomocí tohoto modulu si můžete přizpůsobit detailní chování systému pomocí pravidel pro systémový registr, aktivní procesy a programy.
Herní režim	Při hraní her a používání aplikací běžících v režimu celé obrazovky (fullscreen) se nezobrazí upozornění ani vyskakovací okna a program tak uvolní systémové prostředky pro náročné aplikace.

Funkce ESET Smart Security

Ochrana bankovnictví a online plateb	Dodatečná ochranná vrstva do internetového prohlížeče. Tato vrstva se stará o to, aby vaše osobní data (čísla bankovních účtů, kreditních karet atp.) nebyla v průběhu online transakcí zneužita, resp. nemohly je získat jiné aplikace.
Podpora síťových vzorků	Jedná se o doplněk do ochrany proti botnetu, díky kterému dokážeme rychleji identifikovat a blokovat škodlivou komunikaci pocházející z napadených počítačů nebo na ně směřující.
Inteligentní firewall	Modul firewall kontroluje síťovou komunikaci a chrání počítač před neautorizovaným přístupem.
ESET Antispam	Antispamový modul dokáže filtrovat nevyžádanou poštu (spam), která dnes představuje více než 80 % veškeré e-mailové komunikace.
ESET Anti-Theft	ESET Anti-Theft zvyšuje bezpečnost dat uživatele ve chvíli ztráty nebo

	odcizení počítače. Po aktivaci této technologie bude monitorována podezřelá aktivita na zařízení. Prostřednictvím webového rozhraní můžete zařízení vzdáleně ovládat a v případě jeho ztráty jej označit jako ztracené. Tím ochráníte data v něm uložená.
Rodičovská kontrola	Pomocí kategorií můžete omezit přístup na definované internetové stránky, například stránky s nevhodným obsahem.

Pro správnou funkci všech bezpečnostních funkcí ESET Smart Security musíte mít platnou licenci. Doporučujeme prodloužit si licenci ESET Smart Security v dostatečném předstihu před jejím koncem platnosti.

1.1 Co je nového ve verzi 9?

Uživatelské rozhraní ESET Smart Security bylo po grafické stránce kompletně přepracováno při zachování intuitivního ovládání. ESET Smart Security ve verzi 9 přináší nové funkce a drobná vylepšení:

- **Ochrana bankovnictví a online plateb** – nabízí dodatečnou ochranu při online transakcích.
- **Podpora síťových vzorků** – prostřednictvím síťových vzorků dokážeme rychleji identifikovat a blokovat škodlivou komunikaci pocházející z napadených počítačů nebo na ně směřující.
- **Přepracované uživatelské rozhraní** – grafické rozhraní ESET Smart Security bylo kompletně přepracováno. Nyní je čistější, přehlednější a intuitivnější. Nově jsme přidali také podporu pro jazyky se zápisem doleva jako je Hebrejština a Arabština. Prostřednictvím online nápovědy získáte vždy nejrelevantnější informace k aktuálně zobrazenému dialogovému oknu a nápověda vám pomůže vyřešit váš problém.
- **Rychlejší a spolehlivější instalace** – součástí je naplánovaná automatická kontrola počítače, která se spustí do 20 minut od instalace.

Pro více informací o nových funkcích ESET Smart Security si přečtěte následující článek v ESET Databázi znalostí:
Co je nového v ESET Smart Security 9 a ESET NOD32 Antivirus 9?

1.2 Systémové požadavky

Pro plynulý běh ESET Smart Security by váš systém měl splňovat následující požadavky:

Podporované procesory: Intel® nebo AMD x86-x64
Operační systémy: Microsoft® Windows® 10/8.1/8/7/Vista/XP SP3 32-bit/XP SP2 64-bit/Home Server 2003 SP2 32-bit/ Home Server 2011 64-bit

1.3 Prevence

Při používání počítače, zejména při práci s internetem, je potřeba mít neustále na paměti, že žádný antivirový systém nedokáže zcela odstranit riziko nákazy počítače a útoků. Pro zaručení maximální bezpečnosti a pohodlí je potřeba antivir správně používat a dodržovat několik užitečných pravidel:

Pravidelná aktualizace antivirového systému

Podle statistik z ESET LiveGrid® vznikají denně tisíce nových unikátních infiltrací, které se snaží obejít zabezpečení počítačů a přinést svým tvůrcům zisk. Viroví analytici společnosti ESET tyto hrozby denně analyzují a vydávají aktualizace, které zvyšují úroveň ochrany uživatelů antivirového systému. Při nesprávném nastavení aktualizace se účinnost antivirového systému dramaticky snižuje. Podrobnější informace, jak správně nastavit aktualizace produktu, naleznete v kapitole Nastavení aktualizace.

Stahování bezpečnostních záplat

Tvůrci infiltrací s oblibou využívají chyby v často používaných programech, aby zvýšili účinnost šíření škodlivých kódů. Výrobci většiny programů proto pravidelně vydávají bezpečnostní záplaty, které chyby v produktech opravují. Důležité je stáhnout tyto aktualizaci co nejdříve poté, co byly vydány. Mezi takové programy, které jsou aktualizovány pravidelně, můžeme zařadit například operační systém Windows nebo internetový prohlížeč Internet

Explorer.

Zálohování důležitých dat

Tvůrci infiltrací většinou neberou ohled na potřeby uživatelů. Infiltrace tak mohou způsobit částečnou nebo úplnou nefunkčnost programů, operačního systému nebo poškození dat, někdy dokonce i záměrně. Pravidelné zálohování citlivých a důležitých dat například na DVD nebo externí disk může výrazně usnadnit a urychlit případnou obnovu po pádu systému.

Pravidelná kontrola počítače

Detekci známých i neznámých virů, červů, trojských koní a rootkitů zajišťuje rezidentní štít souborového systému. To znamená, že při každém přístupu k souboru, dojde k jeho kontrole. Přesto doporučujeme pravidelně spouštět úplnou kontrolu počítače alespoň jednou za měsíc, pro zajištění odstranění infiltrací, které pronikly jinými úrovněmi ochrany v době starší virové databáze.

Dodržování základních bezpečnostních pravidel

Jedním z nejužitečnějších a nejúčinnějších bezpečnostních opatření je obezřetnost uživatele. V současnosti vyžaduje většina infiltrací přímé spuštění uživatelem. Proto opatrnost při otevírání souborů vás může ušetřit mnoha problémům a zabránit proniknutí škodlivého kódu do počítače. Zde jsou některé užitečné rady:

- Omezte návštěvy podezřelých stránek, které uživatele bombardují otevíráním oken s reklamními nabídkami apod.
- Dbejte zvýšené opatrnosti při stahování a instalaci volně šiřitelných programů, kodeků apod. Doporučujeme používat pouze ověřené programy a navštěvovat bezpečné internetové stránky.
- Dbejte zvýšené opatrnosti při otevírání příloh e-mailů zvláště u hromadně posílaných zpráv nebo u zpráv od neznámých odesílatelů.
- Nepoužívejte pro běžnou práci na počítači účet s oprávněním Administrátora.

2. Instalace

Instalaci ESET Smart Security můžete provést dvěma způsoby.

- Live installer si můžete stáhnout z internetových stránek společnosti ESET. Live installer je univerzální pro všechny jazykové varianty (při instalaci vyberete jazykovou verzi). Po spuštění se automaticky stáhnou všechny potřebné soubory pro instalaci ESET Smart Security.

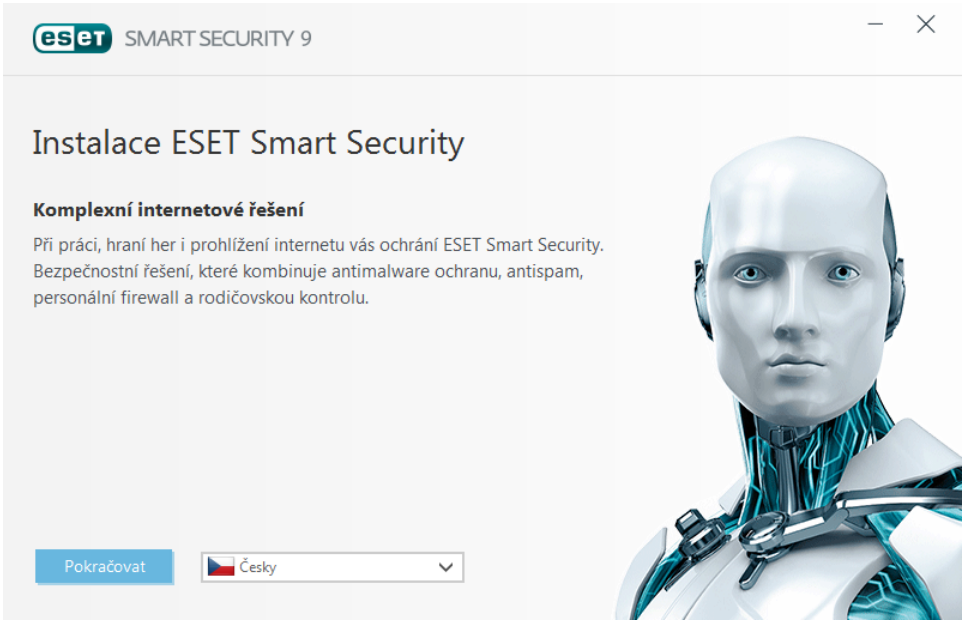
- Offline instalace – tento typ instalace je běžný při instalaci z CD/DVD. Používá soubor *.exe*, který obsahuje všechny instalační soubory, proto je větší než Live installer. Připojení k internetu není potřebné pro dokončení instalace.

Důležité: Před spuštěním instalace ESET Smart Security se ujistěte, že na počítači není nainstalován žádný jiný antivirový program. Současný běh dvou a více antivirových programů na jednom počítači může vést k vzájemné nekompatibilitě, proto doporučujeme odinstalovat všechny ostatní antivirové programy. V ESET Databázi znalostí naleznete nástroje pro odinstalaci nejrozšířenějších antivirových programů.

2.1 Live installer

Po stažení instalačního balíčku *Live installeru*, dvojitým kliknutím pravým tlačítkem myši na stažený soubor spusťte instalaci a postupujte podle pokynů na obrazovce.

Důležité: Pro instalaci je nutné připojení k internetu.



Z rozbalovacího menu vyberte požadovanou jazykovou verzi a klikněte na tlačítko **Instalovat**. Instalace začne za pár okamžiků, po stažení všech potřebných souborů.

Poté, co odsouhlasíte licenční ujednání, budete vyzváni k nastavení **ESET LiveGrid®**. ESET LiveGrid® pomáhá bezprostředně informovat společnost ESET o nových hrozbách a tím chránit zákazníky. Tento systém funguje na principu odeslání podezřelých vzorků do virových laboratoří ESET, kde jsou analyzovány a na základě získaných dat je vytvořena aktualizace virové databáze.

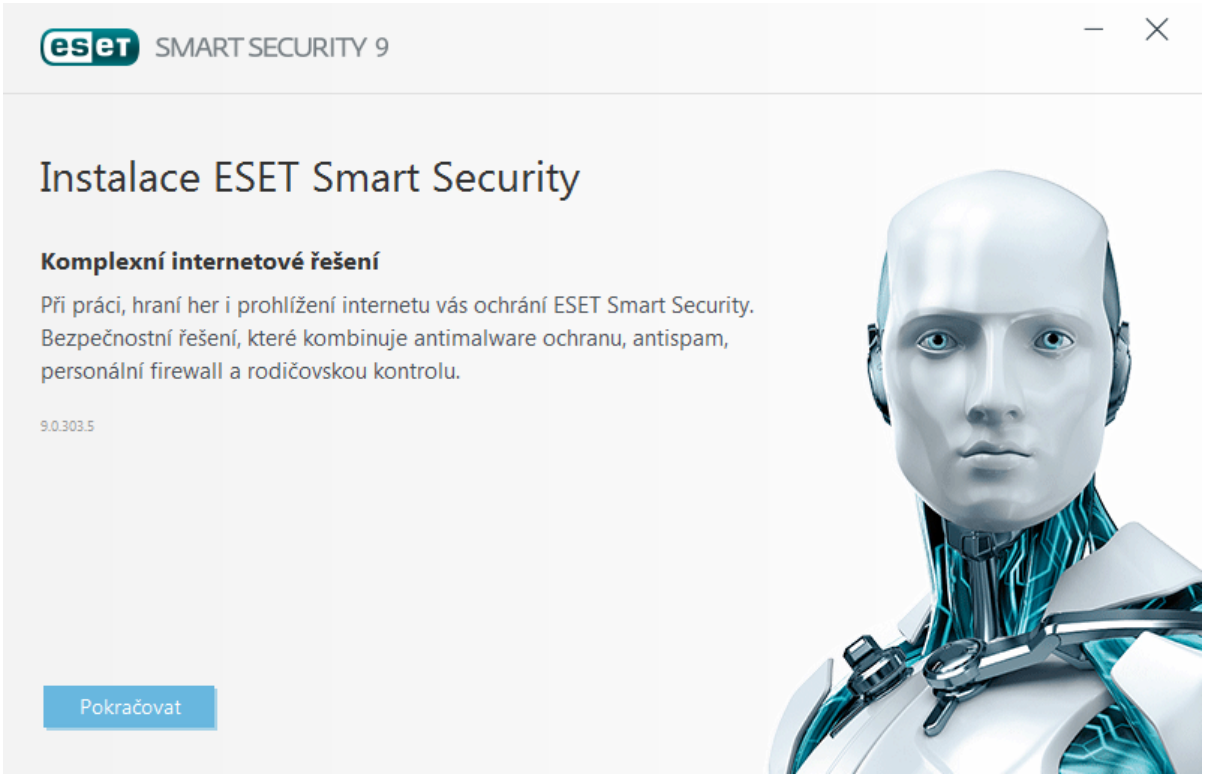
Standardně je vybrána možnost **Chci se zapojit do systému včasného varování ESET LiveGrid® (doporučujeme)** a tato funkce bude po instalaci aktivována.

Dalším krokem je nastavení detekce potenciálně nechtěných aplikací. Potenciálně nechtěné aplikace nemusí být nutně škodlivé, ale mohou negativně ovlivnit chování operačního systému. Více informací naleznete v kapitole Potenciálně nechtěné aplikace.

Klikněte na tlačítko **Instalovat** pro spuštění instalačního procesu.

2.2 Offline instalace

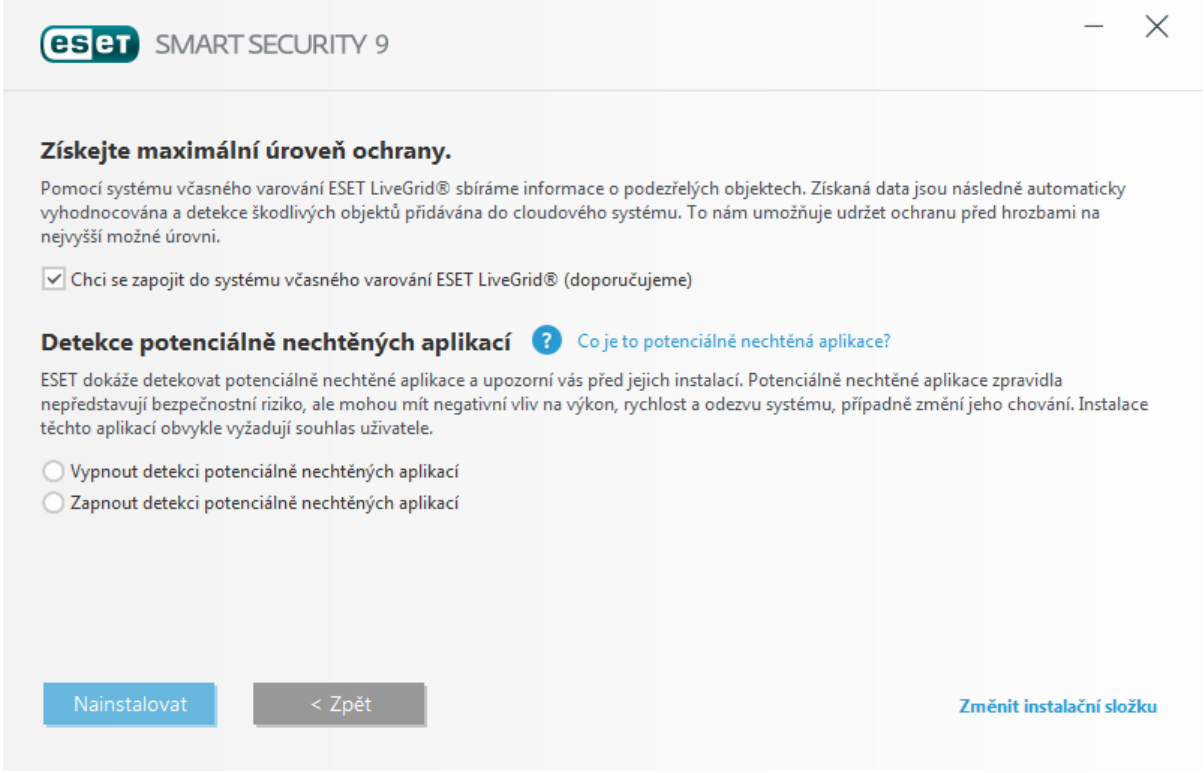
Po spuštění offline instalačního balíčku (.exe) se zobrazí průvodce, který vás provede celým procesem instalace.



Nejprve program zkontroluje, zda není k dispozici novější verze ESET Smart Security. Pokud bude nalezena novější verze budete o tom informováni. Necháte-li zaškrtnutou možnost **Stáhnout a nainstalovat novou verzi**, nová verze produktu se automaticky stáhne a instalace poté bude pokračovat. Tato možnost se zobrazí pouze pokud byla nalezena nová verze.

Klikněte na **Další**, přečtěte si prosím licenční ujednání a odsouhlaste kliknutím na **Souhlasím**. Po přijetí licenčních podmínek bude instalace pokračovat.

Pro více informací o instalačních krocích **ThreatSense** a **Detekci potenciálně nechtěných aplikací** se podívejte do odpovídajících částí kapitoly Live installer.



Možnosti instalace jsou navrženy tak, aby byly vhodné pro většinu uživatelů, proto je není nutné standardně měnit. Přednastavená konfigurace poskytuje výbornou bezpečnost, jednoduchou správu a vysoký výkon systému. **Pokročilé nastavení** je navrženo pro uživatele, kteří mají zkušenosti s úpravou programů a chtějí si změnit nastavení již v průběhu instalace. Klikněte na **Instalovat** pro spuštění instalace a přeskočení Pokročilého nastavení.

2.2.1 Pokročilá instalace

Po vybrání **Pokročilého nastavení** budete vyzváni k výběru umístění instalace. Standardně se program instaluje do složky:

C:\Program Files\ESET\ESET Smart Security

Umístění instalace můžete změnit kliknutím na tlačítko **Procházet...** (nedoporučujeme).

Klikněte na **Další** pro konfiguraci připojení k internetu. Pokud používáte proxy server, musí být správně nastaven, aby fungovaly aktualizace virové databáze. Pokud nevíte, zda pro připojení k internetu používáte proxy server, vyberte možnost **Nastavení podle Internet Exploreru** a klikněte na **Další**. Pokud proxy server nepoužíváte, vyberte **Při připojení nepoužívám proxy server**.

Pro konfiguraci proxy serveru vyberte možnost **Při připojení používám proxy server** a klikněte na tlačítko **Další**. Do pole **Adresa** zadejte IP adresu nebo URL adresu proxy serveru. Pole **Port** slouží k určení portu, na kterém proxy server přijímá spojení (standardně 3128). Pokud proxy server vyžaduje autorizaci, je potřeba vyplnit pole **Přístupové jméno a Heslo**. Proxy server můžete nastavit také podle nastavení Internet Exploreru. Pro nastavení proxy severu tímto způsobem, klikněte na tlačítko **Použít** a potvrďte okno s výzvou.

Vlastní instalace umožňuje definovat chování automatických aktualizací programových komponent. Kliknutím na **Změnit...** přejdete na Rozšířená nastavení.

Pokud nechcete automaticky aktualizovat programové komponenty, vyberte možnost **Neaktualizovat programové komponenty**. Možností **Před aktualizací programových komponent se zeptat uživatele** si vyžádáte potvrzení před stažením a instalací programových komponent. Pro automatické stahování aktualizací programových komponent zajistíte volbou **Vždy aktualizovat programové komponenty**.

Poznámka: Po aktualizaci programových komponent je obvykle vyžadován restart počítače. Doporučujeme vybrat možnost **V případě potřeby, restartovat počítač bez upozornění**.

Dalším krokem instalace je nastavení hesla pro ochranu nastavení programu. Vyberte možnost **Chci nastavení chránit heslem** a zadejte heslo, které bude vyžadováno při každém přístupu k nastavením ESET Smart Security nebo jeho

změně. Pro potvrzení hesla musíte zadat heslo znovu, čímž se předejde možnému překlepu, a poté klikněte na **Další**.

Pro dokončení instalačních kroků **ThreatSense** a **Detekce potenciálně nechtěných aplikací** se podívejte do odpovídajících částí kapitoly Live installer.

Dále vyberte režim filtrování ESET Personálního firewallu, kterých je k dispozici pět. Chování ESET Smart Security Personálního firewallu se mění v závislosti na vybraném režimu. Režimy filtrování mají také vliv na míru interakce uživatele.

Pro vypnutí prvotní kontroly po instalaci odškrtněte možnost **Spustit kontrolu po instalaci**. Pro dokončení instalace klikněte na tlačítko **Instalovat**.

2.3 Známé problémy při instalaci

Pokud se při instalaci produkt ESET vyskytne problém, zkuste řešení najít v Databázi znalostí.

2.4 Aktivace produktu

Po dokončení instalace budete vyzváni k aktivaci produktu.

Produkt můžete aktivovat několika způsoby. Dostupnost jednotlivých metod závisí na zemi a způsobu distribuce (CD/DVD, webové stránky společnosti ESET, apod.).

Pro aktivaci ESET Smart Security klikněte na ikonu v oznamovací oblasti a vyberte možnost **Aktivovat produkt**. Produkt můžete aktivovat také v hlavním okně po kliknutí na záložku **Nápověda a podpora** > **Aktivovat produkt** nebo **Domů** > **Aktivovat produkt**.

K dispozici jsou následující možnosti aktivace:

- **Licenční klíč** – unikátní řetězec znaků ve formátu XXXX-XXXX-XXXX-XXXX-XXXX, který slouží pro identifikaci vlastníka licence a její aktivaci.
- Pokud si chcete produkt ESET Smart Security nejprve vyzkoušet, vyberte možnost **Bezplatná zkušební licence**. Následně budete vyzváni k zadání e-mailové adresy, na kterou obdržíte zkušební údaje. Každý zákazník si může zkušební licenci aktivovat pouze jednou.
- Pokud zatím nemáte žádnou licenci, klikněte na možnost **Zakoupit licenci**. Následně budete přesměrování na webové stránky lokálního distributora ESET.

Pokud máte pouze klasické licenční údaje (uživatelské jméno a heslo), klikněte na možnost **Mám uživatelské jméno a heslo, co mám dělat**. Následně budete přesměrováni na online portál, na kterém si můžete licenční údaje přegenerovat a získat nový licenční klíč.

Po aktivaci produktu na záložce **Nápověda a podpora** > **Základní informace pro technickou podporu** naleznete uživatelské jméno, které se používá pro identifikaci uživatele při komunikaci s technickou podporou společnosti ESET.

2.5 Zadání licenčního klíče

Pro správný chod programu je důležité, aby byl automaticky aktualizován. To je možné pouze tehdy, pokud jste jej aktivovali.

Pokud jste produkt neaktivovali po dokončení instalace programu, můžete tak učinit nyní. V hlavním okně programu klikněte na záložku **Nápověda a podpora**, v pravé části klikněte na **Aktivovat produkt** a do zobrazeného dialogového okna zadejte licenční údaje, které jste obdrželi při nákupu bezpečnostního produktu ESET.

Licenční klíč zadávejte přesně tak, jak je uvedeno na licenčním certifikátu.

- Licenční klíč je Unikátní řetězec znaků ve formátu XXXX-XXXX-XXXX-XXXX-XXXX, který slouží pro identifikaci vlastníka licence a její aktivaci.

Poznámka: Údaje z licenčního e-mailu doporučujeme zkopírovat (CTRL+C) a vložit do programu (CTRL+V). Při

kopírování dejte pozor, abyste navíc nevložili mezeru.

2.6 Aktualizace na novou verzi

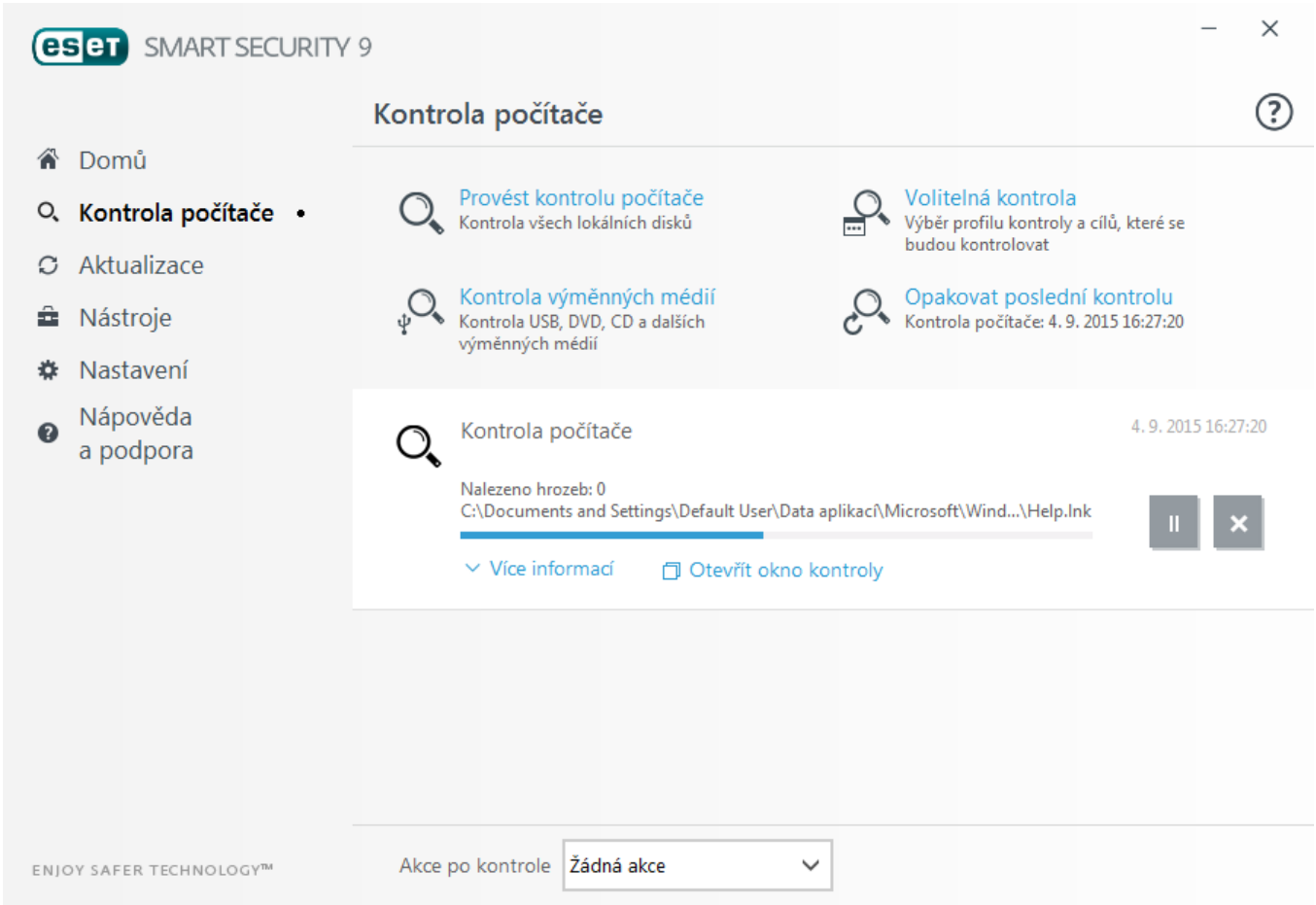
Nové verze ESET Smart Security jsou vydávány pro zdokonalení produktu a opravu chyb, které není možné distribuovat v rámci automatické aktualizace programových modulů. Existuje několik způsobů, jak aktualizovat produkt na novější verzi.

1. Automaticky prostřednictvím aktualizace programu.
   Jelikož se aktualizace programu týká všech uživatelů a může mít významný dopad na systém, je vydávána až po dlouhém období testování na všech operačních systémech v různých konfiguracích. Pokud chcete aktualizovat na nejnovější verzi ihned po jejím vydání, použijte některou z níže uvedených metod.
2. Ručně, v hlavním okně na záložce **Aktualizace** klikněte na **Zkontrolovat aktualizace**.
3. Ručně, stáhněte a nainstalujte přes původní produkt.

2.7 Kontrola počítače po dokončení instalace

Po nainstalování ESET Smart Security se do 20 minut nebo po restartování počítače spustí automatická kontrola počítače.

Kontrolu počítače můžete spustit také kdykoli ručně kliknutím v hlavním okně na záložku **Kontrola počítače** > **Provést kontrolu počítače**. Více informací naleznete v kapitole Kontrola počítače.



3. Začínáme

Tato kapitola poskytuje první seznámení s produktem ESET Smart Security a jeho základním nastavení.

3.1 Seznámení s uživatelským prostředím

Hlavní okno produktu ESET Smart Security je rozděleno na dvě hlavní části. Pravá část slouží k zobrazování informací, přičemž její obsah závisí na vybrané možnosti v levém menu.

Následuje popis jednotlivých záložek hlavního menu v levé části okna:

Domů – v přehledné formě poskytuje informace o stavu ochrany ESET Smart Security,

Kontrola počítače – umožňuje nastavit a spustit tzv. Smart nebo volitelnou kontrolu počítače a kontrolu výměnných médií. Také můžete zopakovat naposledy provedenou kontrolu.

Aktualizace – zobrazuje informace o aktualizacích virové databáze,

Nastavení – obsahuje možnosti nastavení ochrany pro Počítač, Síť a Web a mail.

Nástroje – zajišťuje přístup k protokolům, statistikám ochrany, sledování aktivity, spuštěným procesům, plánovači, karanténě, síťovým spojením, nástroji ESET SysInspector a ESET SysRescue pro vytvoření záchranného CD. Dále zde naleznete možnost pro odeslání vzorku k analýze do virových laboratoří společnosti ESET.

Nápověda a podpora – poskytuje přístup k nápovědě, ESET Databázi znalostí a webové stránce společnosti ESET. Dále zde můžete přímo vytvořit dotaz na technickou podporu, v dolní části okna naleznete diagnostické nástroje a informace o aktivaci produktu.

Na záložce **Stav ochrany** jsou zobrazeny informace o bezpečnosti a úrovni ochrany počítače.

Zelená ikona a informace **Maximální ochrana** znamená, že je zajištěna maximální úroveň ochrany.

V tomto okně dále naleznete odkazy na často používané funkce ESET Smart Security a informace o poslední

aktualizaci virové databáze.

Co dělat, pokud systém nepracuje správně?

Při plné funkčnosti ochrany má ikona Stavu ochrany zelenou barvu. V opačném případě je barva červená nebo žlutá a není zajištěna maximální ochrana. Zároveň jsou na záložce **Domů** zobrazeny bližší informace o stavu jednotlivých modulů a návrh na možné řešení problému pro obnovení maximální ochrany. Stav jednotlivých modulů můžete změnit kliknutím na záložku **Nastavení** a vybráním požadovaného modulu.

Červená barva stavu ochrany a informace Není zajištěna maximální ochrana signalizuje kritické problémy. Ochrana vašeho systému tak není zajištěna v plné míře. Možné příčiny jsou:

- **Produkt není aktivován** – ESET Smart Security můžete aktivovat kliknutím na záložku **Domů** a vybráním možnosti **Aktivovat plnou verzi** nebo **Zakoupit nyní**.
- **Virová databáze je zastaralá** – tato chyba se zobrazí po neúspěšném kontaktování serveru při pokusu o aktualizaci virové databáze. V takovém případě doporučujeme zkontrolovat nastavení aktualizací. Nejčastějším důvodem neaktivovaný produkt nebo chybně nastavené připojení k internetu.
- **Vypnutá antivirová a antispyware ochrana** – antivir a antispyware ochranu znovu zapněte kliknutím na **Spustit všechny moduly antiviru a antispyware**.
- **Vypnutý ESET Personální firewall** – na tento problém jste upozorňováni také bezpečnostním oznámením vedle položky **Síť** na pracovní ploše. Znovu zapnout ochranu můžete kliknutím na **Zapnout firewall**.
- **Vypršela licence produktu** – v tomto případě ikona ochrany změní barvu na červenou. Program nebude možné od této chvíle aktualizovat. Pro prodloužení licence doporučujeme řídit se instrukcemi zobrazenými v okně s upozorněním.

Žlutá barva stavu ochrany znamená částečné problémy. Například problémy s aktualizací programu nebo blížící se datum vypršení licence.
Možné důvody jsou:

- **Upozornění Anti-Theft diagnostiky** – toto zařízení není optimalizováno pro ESET Anti-Theft. Například není

vytvořen Fantom účet, ale bezpečnostní funkce automaticky se automaticky spustí, pokud bude zařízení označeno jako ztracené. Pro použití funkce Optimalizace je potřeba vytvořit Fantom účet ve webovém rozhraní ESET Anti-Theft.

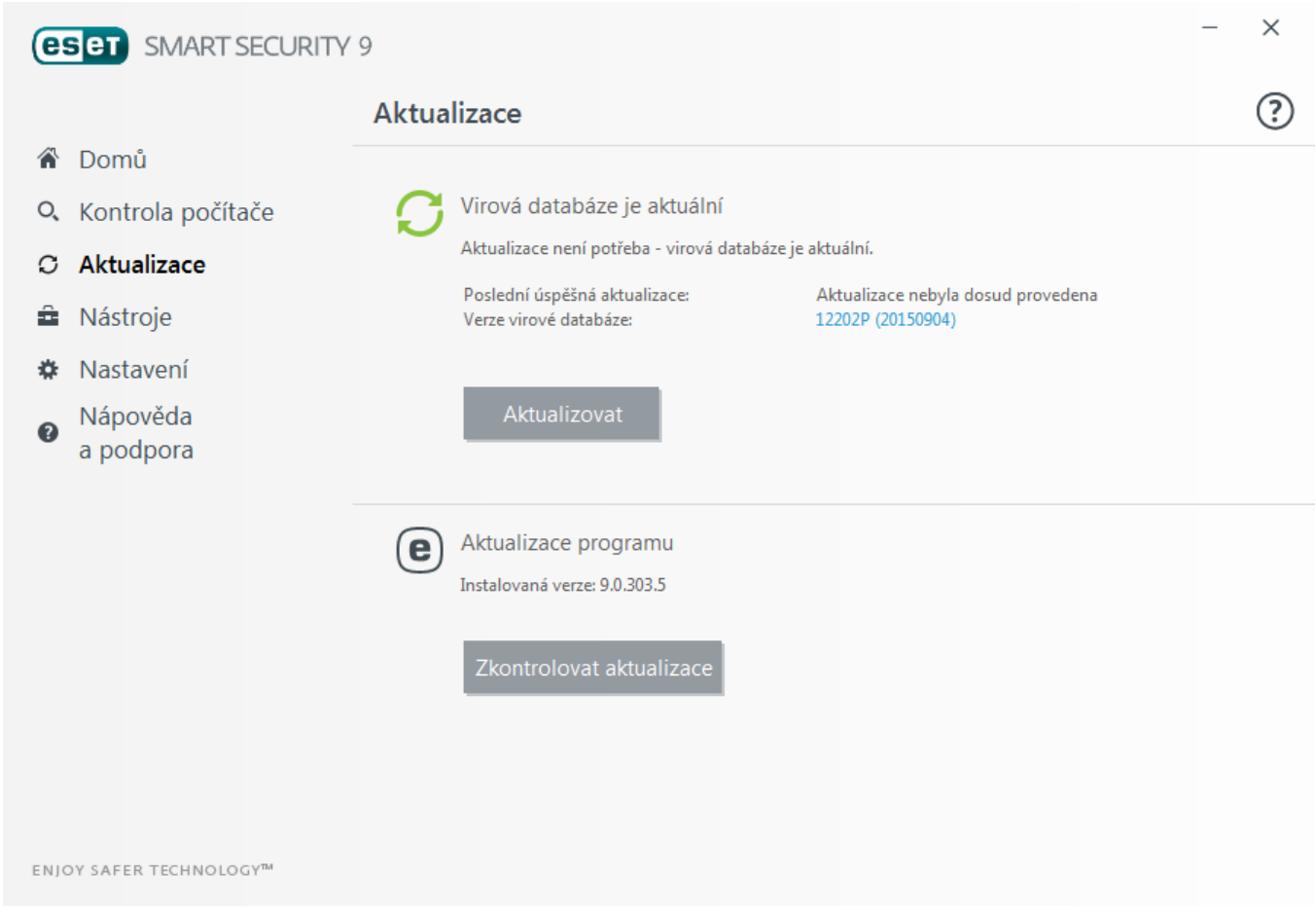
- **Je zapnutý herní režim** – zapnutí Herního režimu představuje potenciální bezpečnostní riziko. Tato funkce zakáže zobrazování všech oken s upozorněním a pozastaví všechny naplánované úlohy.
- **Blíží se konec platnosti licence** – v tomto případě ikona ochrany změní barvu na žlutou a zobrazí se varovné hlášení. Poté, co licence vyprší, se program nebude aktualizovat a ikonka ochrany změní barvu na červenou.

V případě, že není možné problém vyřešit, klikněte v hlavním okně programu na záložku **Nápověda a podpora** a zobrazte nápovědu nebo přejděte do ESET Databáze znalostí. Pokud i přesto budete potřebovat pomoc, můžete odeslat dotaz na technickou podporu. Specialisté technické podpory ESET reagují rychle a pomáhají při řešení problémů.

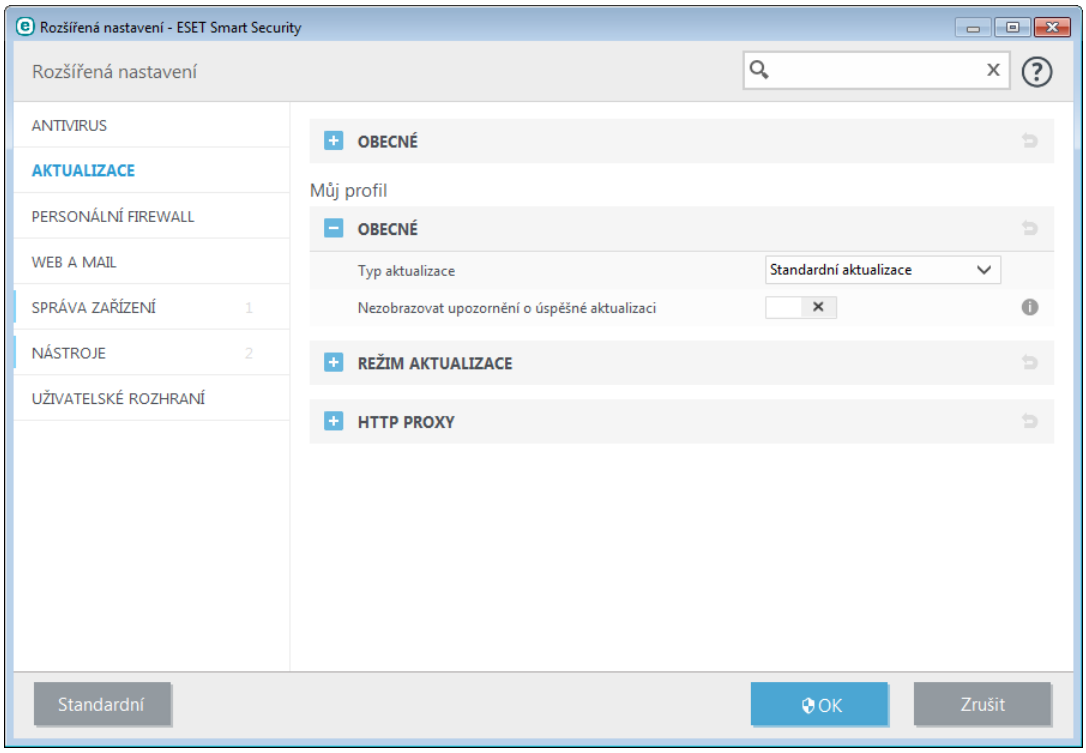
3.2 Aktualizace

Aktualizace virové databáze a programových komponent je důležitá pro zajištění komplexní ochrany před škodlivým kódem. Jejímu nastavení a funkčnosti je proto potřeba věnovat zvýšenou pozornost. Pro zkontrolování dostupnosti aktualizace virové databáze klikněte v hlavním menu na záložku **Aktualizace** a následně na tlačítko **Aktualizovat**.

Poznámka: Pokud jste produkt do této chvíle neaktivovali, budete k tomu vyzváni právě teď.



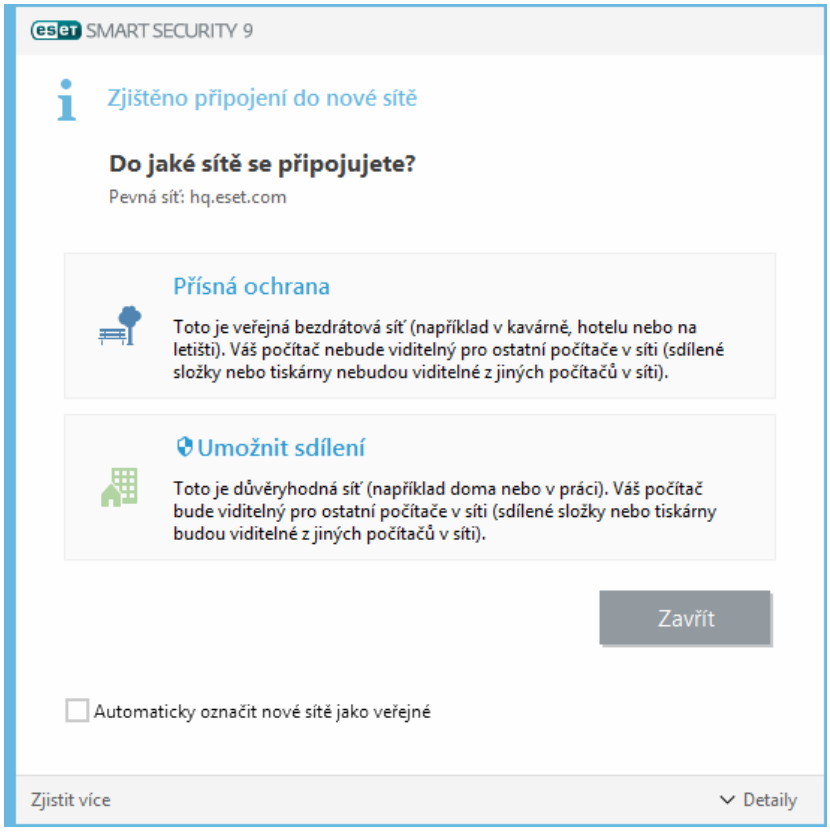
Pro konfiguraci podrobných nastavení aktualizace jako režim aktualizace, nastavení přístupu přes proxy atp. přejděte do rozšířeného nastavení (dostupné po stisknutí **klávesy F5**) na záložku **Aktualizace**.



3.3 Nastavení důvěryhodné zóny

Pro ochranu počítače v síťovém prostředí je nezbytné nastavit důvěryhodnou zónu. Jejím nakonfigurováním můžete umožnit ostatním uživatelům přístup k vašemu počítači. Kliknutím na **Nastavení** > **Síť** > **Změnit režim ochrany počítače v síti...** se zobrazí dialogové okno s možností výběru režimu ochranu počítače v síti.

Automatická detekce důvěryhodné zóny se provede po nainstalování ESET Smart Security a kdykoli při připojení počítače do nové sítě. Proto není obvykle nutné definovat důvěryhodnou zónu, protože se standardně se při detekci nové zóny zobrazí dialogové okno s možností definovat úroveň zabezpečení.



Varování: Nesprávným nastavením důvěryhodné zóny vystavujete počítač ohrožení.

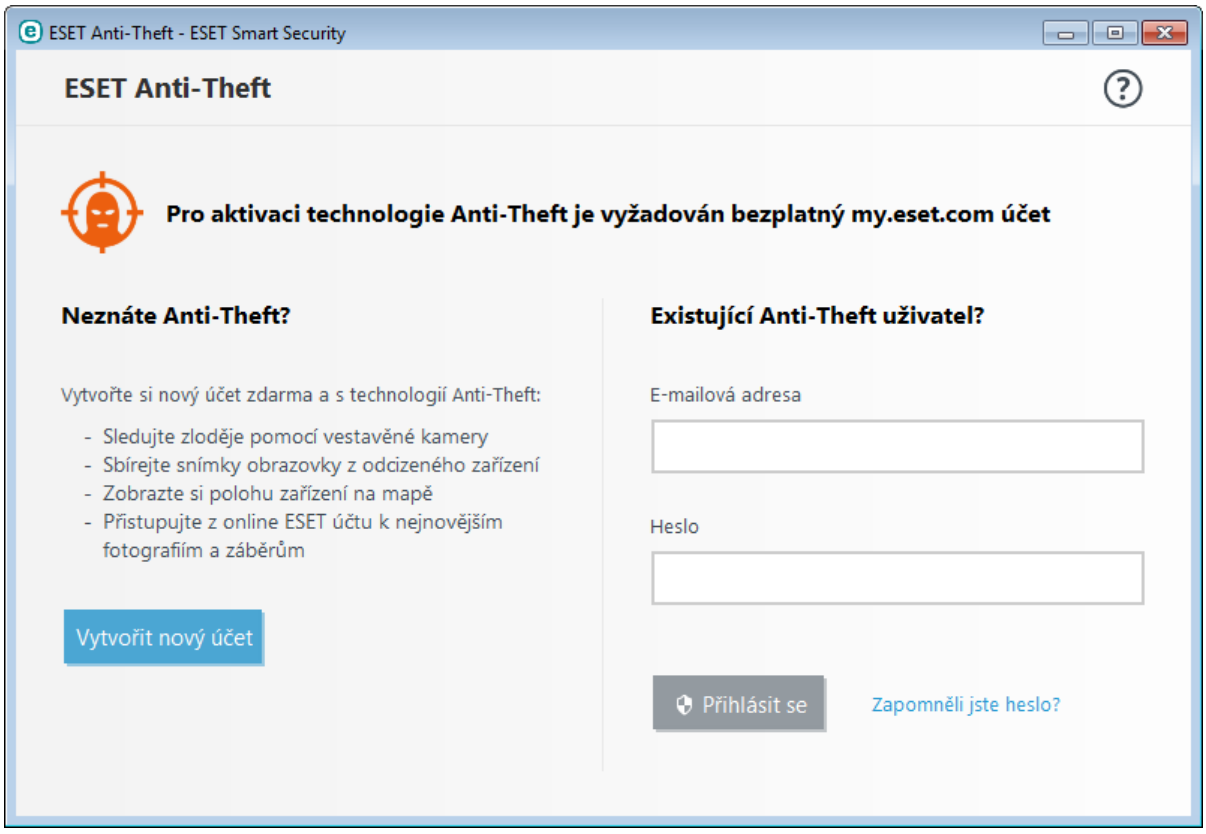
Poznámka: Standardně je počítačům z důvěryhodné zóny povolen přístup ke sdíleným souborům a tiskárnám, povolena příchozí RPC komunikace a je dostupná služba sdílení pracovní plochy.

Pro více informací o této funkci přejděte do Databáze znalostí.

3.4 Anti-Theft

Pro ochranu počítače v případě ztráty nebo odcizení postupujte podle následujících kroků pro registraci počítače do systému ESET Anti-Theft.

1. Po úspěšné aktivaci produktu klikněte na **Zapnout Anti-Theft** pro aktivování funkcí ESET Anti-Theft a registraci počítače.



2. Pokud se na záložce **Domů** v hlavním okně ESET Smart Security zobrazuje informace **ESET Anti-Theft je dostupný**, zvažte aktivaci této funkce pro daný počítač. Klikněte na **Zapnout ESET Anti-Theft** pro propojení počítače s modulem ESET Anti-Theft.
3. V hlavním okně programu přejděte na záložku **Nastavení**, poté klikněte na **ESET Anti-Theft** a postupujte dle pokynů na obrazovce.

Poznámka: ESET Anti-Theft není dostupný na Microsoft Windows Home Server.

Více informací o funkci ESET Anti-Theft a propojení s počítačem naleznete v online nápovědě k portálu my.eset.com.

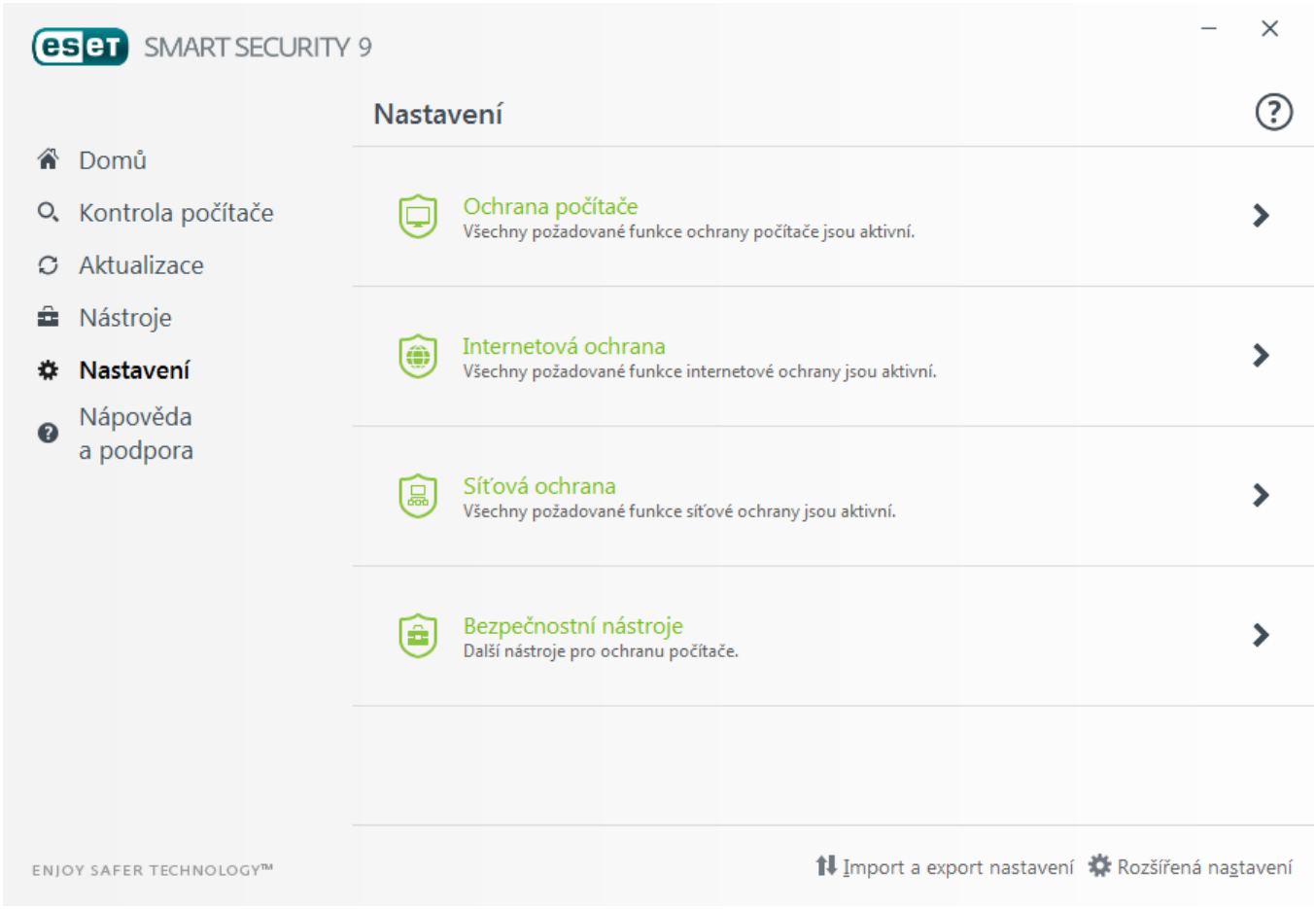
3.5 Nástroje Rodičovské kontroly

Pokud jste aktivovali **Rodičovskou kontrolu** v ESET Smart Security, musíte také nastavit, pro které účty bude kontrola aktivní.

Pokud je Rodičovská kontrola aktivní, ale nevybrali jste žádného uživatele, na záložce **Domů** hlavního okna se zobrazí informace **Rodičovská kontrola není nastavena**. Klikněte na **Nastavit pravidla nyní** a přejděte do kapitoly Rodičovská kontrola pro získání informací, jak vytvořit specifické omezení pro ochranu dětí před potenciálně pohoršujícím obsahem.

4. Práce s ESET Smart Security

Na záložce **Nastavení** můžete konfigurovat úroveň ochrany počítače a sítě.



Záložka **Nastavení** obsahuje následující sekce:

Ochrana počítače
Internetová ochrana
Síťová ochrana
Bezpečnostní nástroje

V sekci **Ochrana počítače** můžete zapnout nebo vypnout následující moduly:

- **Rezidentní ochrana souborového systému** – všechny soubory jsou kontrolovány v momentě, kdy je vytvoříte, otevřete nebo spustíte,
- **HIPS** – systém HIPS monitoruje události uvnitř operačního systému a reaguje na ně na základě pravidel předdefinovaných pravidel společností ESET,
- **Herní režim** – po aktivaci herního režimu vás ESET nebude obtěžovat bublinovými upozorněními a sníží zátěž na CPU. Zároveň hlavní okno změní barvu na oranžovou a upozorní vás na potenciální bezpečnostní riziko.
- **Anti-Stealth ochrana** – detekuje nebezpečné programy jako rootkity, které jsou po svém spuštění neviditelné pro operační systém, a další ochranné mechanismy a aplikace.

V sekci **Internetová ochrana** můžete zapnout nebo vypnout následující moduly:

- **Ochrana přístupu na web** – pokud je zapnuta, veškerá komunikace přes HTTP nebo HTTPs je kontrolována na přítomnost škodlivého kódu,
- **Ochrana poštovních klientů** – zabezpečuje kontrolu poštovní komunikace přijímané prostřednictvím POP3 a IMAP protokolu,
- **Antispamová ochrana** – kontroluje na přítomnost nevyžádané pošty.
- **Anti-Phishingová ochrana** – chrání vás před pokusy o získání hesel, bankovních dat a dalších důvěrných informací z webových stránek, které se tváří jako legitimní.

V sekci **Ochrana sítě** můžete zapnout nebo vypnout Personální firewall, ochranu proti síťovým útokům (IDS) a ochranu proti botnetu.

V sekci **Bezpečnostní nástroje** můžete zapnout nebo vypnout následující součásti:

- Ochrana bankovnictví a online plateb
- Rodičovská kontrola
- Anti-Theft

Rodičovská kontrola umožňuje blokovat webové stránky, které mohou obsahovat nevhodný obsah. Kromě toho jako rodiče můžete zakázat přístup na 40 předdefinovaných kategorií webových stránek, které jsou dále rozděleny na více než 140 podkategorií.

Pro dočasné deaktivování konkrétního modulu klikněte na zelený přepínač . Mějte na paměti, že tím dojde ke snížení úrovně ochrany počítače. Pro znovu zapnutí ochrany vypnutého bezpečnostního modulu klikněte na červený přepínač pro znovu aktivování konkrétního modulu.

Poznámka: Pokud vypnete jednotlivý bezpečnostní modul pomocí tohoto způsobu, bude znovu zapnut po restartování počítače.

Pro přístup do detailního nastavení konkrétního modulu klikněte na ozubené kolečko .

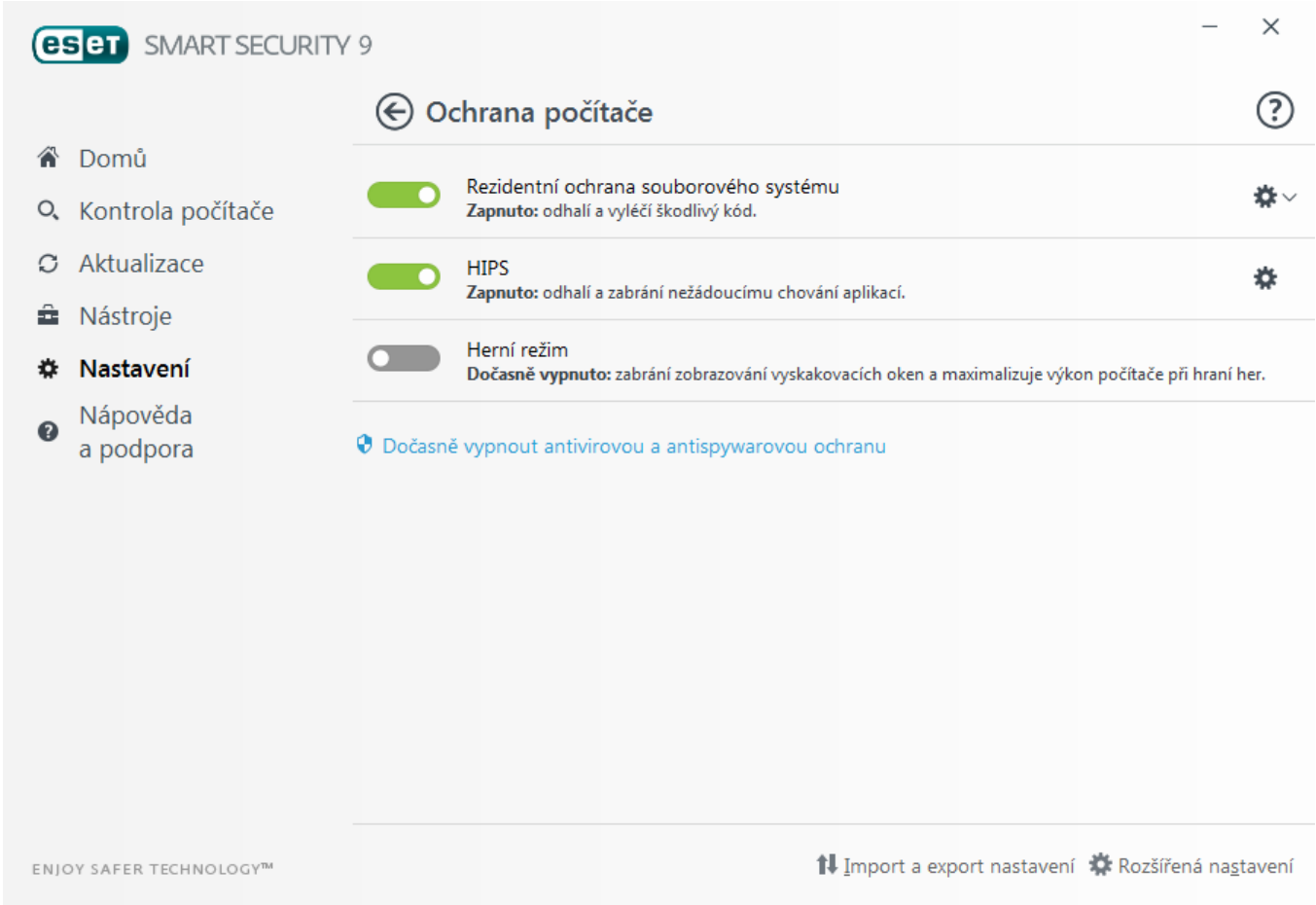
Další možnosti naleznete v dolní části okna. Pro načtení již existující konfigurace z *.xml* konfiguračního souboru nebo pro uložení aktuálního nastavení do souboru klikněte na **Import a export nastavení**. Pro více informací přejděte do kapitoly Import a export nastavení.

Pokud chcete zobrazit detailní nastavení programu, klikněte na tlačítko **Rozšířená nastavení** nebo stiskněte klávesu **F5**.

4.1 Ochrana počítače

V sekci **Nastavení** > **Ochrany počítače** naleznete jednotlivé moduly ochrany počítače Pro dočasné vypnutí jednotlivých modulů použijte přepínač . Mějte na paměti, že tímto můžete snížit úroveň zabezpečení počítače. Detailní nastavení konkrétních modulů se zobrazí po kliknutí na ozubené kolečko .

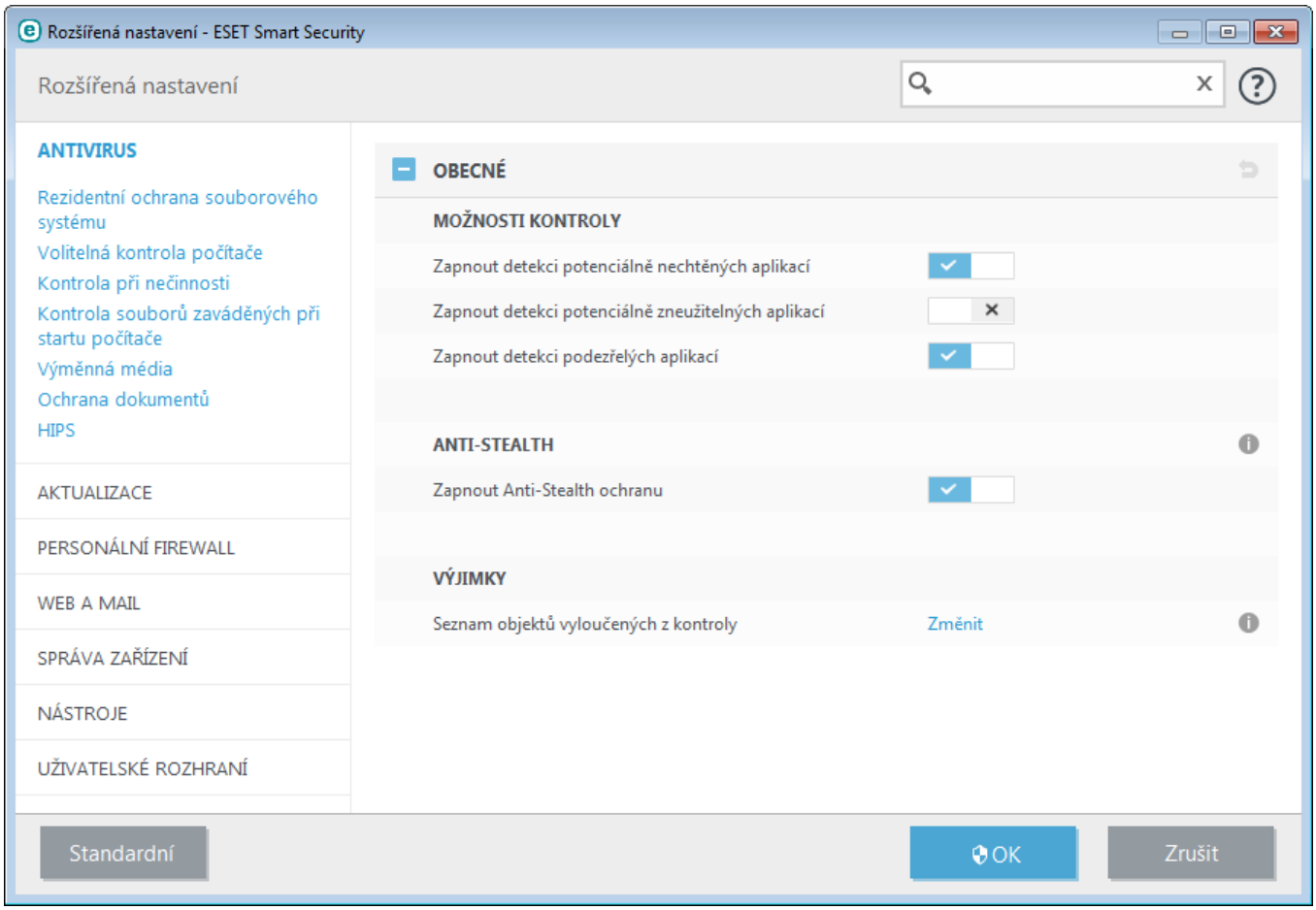
Pro vytvoření výjimek klikněte na ozubené kolečko na řádku rezidentní ochrana souborového systému a vyberte možnost Upravit výjimky....



Dočasně vypnout antivirovou a antispywarovou ochranu – okamžitě vypne všechny moduly antivirové a antispywarové ochrany. Po kliknutí se zobrazí dialogové okno, ve kterém můžete vybrat z rozbalovacího menu časový interval, po který bude rezidentní ochrana vypnuta. Klikněte na **OK** pro potvrzení.

4.1.1 Antivirus

Antivirus a antispyware zajišťuje komplexní ochranu před nebezpečnými programy ohrožujícími systém. Zahrnuje kontrolu souborů, e-mailů a internetové komunikace. V případě zjištění škodlivého kódu jej modul Antivir dokáže eliminovat zablokováním, následným vyléčením, odstraněním nebo přesunutím do karantény.



V možnostech kontroly, které jsou společné pro všechny moduly (např. Rezidentní ochrana souborového serveru, Ochrana přístupu na web,...), můžete zapnout nebo vypnout následující detekci:

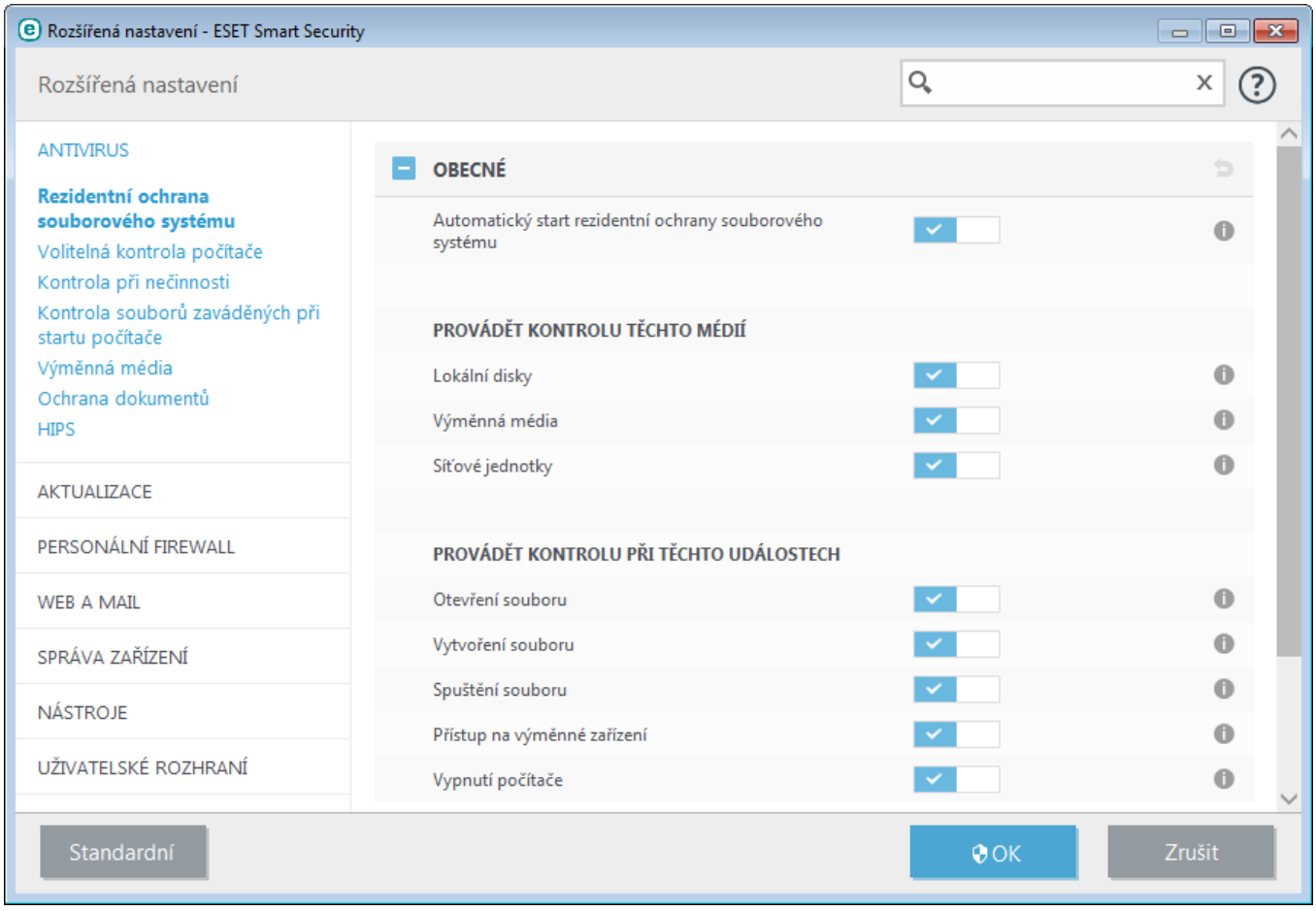
- **Potenciálně nechtěné aplikace** nemusí být nutně škodlivé, v každém případě však mohou mít negativní dopad na výkon počítače.
  Více informací o tomto typu aplikací naleznete ve slovníku pojmů.
- **Potenciálně zneužitelné aplikace** jsou legitimní komerční aplikace, které mohou být zneužity ke škodlivé činnosti. Příkladem mohou být programy pro vzdálené připojení, aplikace k odšifrování hesel a keyloggery (programy, které zaznamenávají zadané znaky na klávesnici). Tato možnost je standardně vypnuta.
  Více informací o tomto typu aplikací naleznete ve slovníku pojmů.
- **Potenciálně podezřelé aplikace** jsou programy, které používají pro kompresi packery nebo jiné ochranné mechanismy zabraňující detekci. Takové typy ochranných mechanismů jsou velice často zneužívány autory škodlivého kódu.

Technologie Anti-Stealth je sofistikovaný systém pro detekci nebezpečných programů například rootkitů, které jsou po svém spuštění neviditelné pro operační systém a bezpečnostní aplikace.

Prostřednictvím **výjimek** můžete vyloučit konkrétní soubory nebo složky z kontroly. Výjimky však doporučujeme vytvářet pouze v ojedinělých případech. Jejich vytvoření může být užitečné například v případě, kdy nechcete kontrolovat velké soubory (databáze, zálohy, ISO soubory atp.), jejichž kontrola zpomaluje systém nebo způsobuje konflikt s jinou aplikací. Pro více informací přejděte do kapitoly výjimky.

4.1.1.1 Rezidentní ochrana souborového systému

Rezidentní ochrana kontroluje veškeré dění v počítači. Všechny soubory, které se v počítači otevírají, vytvářejí a spouštějí jsou kontrolovány na přítomnost infiltrace. Rezidentní ochrana se spouští automaticky při startu systému.



Standardně se rezidentní ochrana spustí vždy při startu operačního systému. Ve zvláštních případech (například pokud dochází ke konfliktu s jiným rezidentním programem), je možné spuštění rezidentní ochrany zastavit odškrtnutím možnosti **Automatický start rezidentní ochrany souborového systému** v **Rozšířeném nastavení** na záložce **Rezidentní ochrana souborového systému** > **Obecné**.

Kontrola médií

Standardně je nastavena kontrola všech typů médií:

Lokální disky – lokální pevné disky v počítači,
Výměnná média – diskety, CD, DVD, USB klíče, Bluetooth zařízení a další,
Síťové disky – namapované síťové disky.

Doporučujeme ponechat toto nastavení. Změnu doporučujeme pouze ve zvláštních případech, např. pokud při kontrole určitého média dochází k výraznému zpomalení.

Kontrola při událostech

Standardně jsou soubory kontrolovány při otevírání, spouštění a vytváření. Tato nastavení doporučujeme ponechat pro zajištění maximální možné ochrany počítače:

- **Otevření souboru** – zapne nebo vypne kontrolu souborů při přístupu a otevírání,
- **Vytvoření souboru** – zapne nebo vypne kontrolu vytvářených nebo upravovaných souborů,
- **Spuštění souboru** – zapne nebo vypne kontrolu souborů při jejich spouštění,
- **Přístup k výměnnému médiu** – zapne nebo vypne kontrolu souborů, které přistupují k výměnným zařízením,
- **Vypnutí počítače** – zapne nebo vypne kontrolu souborů, které vyvolaly vypnutí systému.

Rezidentní ochrana kontroluje všechny typy médií a kontrola je prováděna při různých událostech jako je přístup k

souboru. Při kontrole jsou používány detekční metody technologie ThreatSense (ty jsou popsány v kapitole Nastavení skenovacího jádra ThreatSense). Chování rezidentní ochrany může být odlišné u nově vytvářených než existujících souborů. Například, pro nově vytvářené soubory můžete nastavit hlubší úroveň kontroly.

Pro zajištění minimálních systémových nároků, nejsou již dříve kontrolované soubory znovu kontrolovány (pokud nebyly změněny). Soubory jsou opět kontrolovány pouze po každé aktualizaci virové databáze. Toto chování můžete přizpůsobit pomocí **Smart optimalizace**. Pokud je tato funkce zakázána, všechny soubory jsou kontrolovány vždy, když se k nim přistupuje. Pokud chcete možnosti kontroly upravit, otevřete **Rozšířená nastavení** (stisknutím klávesy F5 v hlavním okně programu), přejděte na záložku **Antivir** > **Rezidentní ochrana souborového systému**. Dále přejděte na záložku **Parametry skenovacího jádra ThreatSense** > **Ostatní** a aktivujte nebo vypněte možnost **Používat Smart optimalizaci**.

4.1.1.1.1 Rozšířená nastavení kontroly

Doplňující parametry ThreatSense pro vytvořené a změněné soubory – pravděpodobnost napadení nově vytvořených nebo upravených souborů je vyšší než u existujících souborů. To je důvod, proč program tyto soubory kontroluje s přidanými parametry. Společně s kontrolou založenou na porovnávání vzorků je využívána pokročilá heuristika, čímž se výrazně zvyšuje úroveň detekce, i když škodlivý kód ještě není znám před vydáním aktualizace virové databáze. Kromě nově vytvářených souborů se kontrolují také samorozbalovací soubory (.sfx) a runtime archivy (interně komprimované spustitelné soubory). Standardně jsou archivy kontrolovány do 10 úrovní vnoření bez ohledu na jejich velikost. Pro změnu kontroly archivů odškrtněte možnost **Standardní nastavení archivů.**

Doplňující parametry ThreatSense pro spouštěné soubory

Rozšířená heuristika pro spouštěné soubory – standardně se Rozšířená heuristika se používá pro spouštěné soubory. Pokud je aktivní, důrazně doporučujeme ponechat zapnutou také Smart optimalizaci a ESET LiveGrid® pro snížení dopadu na výkon systému.

Rozšířená heuristika při spuštění souboru z výměnných médií – rozšířená heuristika emuluje kód aplikace ve virtuálním prostředí a vyhodnotí chování aplikace ještě předtím, než je povoleno aplikaci spuštění z výměnného média.

4.1.1.1.2 Úrovně léčení

Rezidentní ochrana pracuje ve třech režimech léčení (pro jejich zobrazení klikněte na záložku **Rezidentní ochrana souborového systému** > **Parametry skenovacího jádra ThreatSense**).

Neléčit – infikované soubory nebudou automaticky léčeny. Při detekci se zobrazí varovné okno s možností výběru akce, která se má provést. Tato úroveň je navržena pro pokročilé uživatele, kteří vědí, jak postupovat v případě infiltrace.

Standardní úroveň léčení – program se pokusí infikované soubory automaticky léčit, nebo odstranit na základě předdefinované akce (v závislosti na typu infiltrace). Informace o detekci a odstranění infikovaného souboru je zobrazena informační bublinou v pravém dolním rohu obrazovky. Pokud program nedokáže automaticky vybrat správnou akci, zobrazí se okno s možností výběru akce. Možnost výběru akce se zobrazí také v případě, když se předdefinovanou akci nepodaří provést.

Přísné léčení – program vyléčí nebo odstraní všechny infikované soubory. Výjimku tvoří systémové soubory. Pokud je nelze vyléčit, zobrazí se výběr akce, která se má provést.

Varování: Při detekci infiltrace v archivu, bude při standardním a přísném léčení odstraněn celý archiv. Při standardním léčení bude archiv odstraněn, pouze pokud obsahuje samotný soubor s infiltrací. Při **přísném léčení** bude archiv odstraněn i v případě, že kromě infiltrace obsahuje další korektní soubory.

4.1.1.1.3 Kdy měnit nastavení rezidentní ochrany

Rezidentní ochrana je klíčovým modulem zabezpečujícím ochranu počítače. Proto je potřeba být při změnách nastavení obezřetný. Rezidentní ochranu doporučujeme měnit pouze ve specifických případech.

Po instalaci ESET Smart Security jsou veškerá nastavení optimalizována pro zajištění maximální bezpečnosti systému. Standardní nastavení můžete kdykoliv obnovit kliknutím na tlačítko **Standardní**, které se nachází v okně **Rezidentní ochrana souborového systému** v pravém dolním rohu (**Rozšířená nastavení** > **Antivirus** > **Rezidentní ochrana souborového systému**).

4.1.1.1.4 Ověření funkčnosti rezidentní ochrany

Pro ověření, zda je rezidentní ochrana funkční a detekuje viry, je možné použít testovací soubor z webových stránek eicar.com. Jedná se o soubor, který je detekován všemi antivirovými programy a byl vytvořen společností EICAR (European Institute for Computer Antivirus Research) pro testování funkčnosti antivirových programů. Soubor **eicar** je dostupný ke stažení na adrese http://www.eicar.org/download/eicar.com.

Poznámka: Před kontrolou rezidentní ochrany je nutné vypnout firewall. Pokud je firewall zapnutý, soubor je detekován již během stahování, předtím než se může uložit do souborového systému kontrolovaného rezidentní ochranou.

4.1.1.1.5 Co dělat, když nefunguje rezidentní ochrana

V této kapitole jsou popsány problémové stavy, které mohou nastat v případě rezidentní ochrany. Je zde také uvedeno jak postupovat při řešení problémů

Rezidentní ochrana je vypnutá

Pokud byla rezidentní ochrana nedopatřením vypnuta uživatelem, je potřeba ji znovu aktivovat. Opětovné zapnutí je možné kliknutím na záložku **Nastavení** v hlavním okně programu a kliknutím na **Rezidentní ochrana souborového systému**.

Pokud se rezidentní ochrana nespouští při startu operačního systému, pravděpodobně byla vypnuta možnost **Automatický start rezidentní ochrany**. Pro zapnutí této možnosti přejděte na Rozšířená nastavení (dostupná po stisknutí klávesy F5 v hlavním okně programu) a kliknutím na záložku **Počítač** > **Antivirus a antispyware** > **Rezidentní ochrana souborového systému**. V části **Pokročilé** se ujistěte, že je zaškrtnuta možnost **Automatický start rezidentní ochrany**.

Rezidentní ochrana nedetekuje a neléčí infiltrace

Ujistěte se, zda nemáte nainstalován další antivirový program. Mezi dvěma rezidentními ochranami může docházet ke konfliktu. Proto doporučujeme všechny ostatní antivirové programy odinstalovat, před instalací produktu ESET.

Rezidentní ochrana se nespouští při startu

Pokud se rezidentní ochrana nespouští při startu systému ani po aktivování možnosti **Automatický start rezidentní ochrany**, zřejmě dochází ke konfliktu s jiným programem. V takovém případě doporučujeme kontaktovat technickou podporu společnosti ESET.

4.1.1.2 Volitelná kontrola počítače

Důležitou součástí ESET Smart Security je tzv. volitelná kontrola (On-demand), která umožňuje vlastní kontrolu pevných disků, jednotlivých složek a souborů v počítači. Z bezpečnostního hlediska je žádoucí, aby kontrola počítače byla spouštěna nejen při podezření na infikované soubory, ale v rámci prevence i průběžně. Hloubkovou kontrolu pevného disku doporučujeme provádět v určitých časových intervalech, aby byly detekovány případné viry, které v době zápisu na disk nebyly zachyceny Rezidentní ochranou. Taková situace může nastat, pokud byla rezidentní ochrana v té době vypnutá nebo virová databáze zastaralá případně soubor v době zápisu na disk program nebyl vyhodnocen jako vir.

K dispozici jsou dva typy kontroly počítače. **Smart kontrola** rychle prohledá systém a nevyžaduje nastavovat žádné další parametry kontroly. **Volitelná kontrola** umožňuje výběr z předdefinovaných profilů kontroly a cílů kontroly.

Více informací o procesu kontroly naleznete v kapitole Průběh kontroly.

Provést kontrolu počítače

Smart kontrola slouží pro rychlé spuštění kontroly počítače a automaticky léčí nebo odstraňuje infikované soubory a nevyžaduje interakci uživatele. Výhodou Smart kontroly je snadná obsluha, kdy není nutné cokoli dalšího konfigurovat. Smart kontrola zkontroluje všechny soubory na lokálních jednotkách a automaticky je vyléčí nebo odstraní. Úroveň léčení je nastavena na standardní úroveň. Více informací o typech léčení se dozvíte v kapitole Léčení.

Volitelná kontrola

Volitelná kontrola umožňuje výběr z předdefinovaných profilů kontroly a cílů kontroly. Výhodou Volitelné kontroly je možnost přizpůsobit parametry kontroly. Nastavenou konfiguraci můžete uložit do uživatelských profilů, které se dají využít při opakované kontrole.

Pro výběr cílů kontroly klikněte na **Kontrola počítače** > **Vlastní kontrola** a z rozbalovacího menu vyberte **Cíle kontroly** nebo je vyberte ručně ze stromové struktury. Cíle kontroly můžete definovat také přímým zadáním cesty k souboru nebo složce. Pokud chcete spustit pouze kontroly systému, a neléčit případné infiltrace, zaškrtněte možnost **Zkontrolovat bez léčení**. K dispozici jsou tři úrovně léčení, které můžete definovat po kliknutí na **Nastavit...** > **Parametry skenovacího jádra ThreatSense** > **Léčení**.

Provádění volitelné kontroly s vlastními parametry je určeno pokročilým uživatelům, kteří již mají zkušenosti s používáním antivirových programů.

Kontrola výměnných médií

Podobně jako kontrola počítače – spustí rychlou kontrolu výměnných médií (CD/DVD/USB), které jsou aktuálně připojené k počítači. To může být užitečné ve chvíli, kdy si přeje zkontrolovat obsah připojeného USB zařízení k počítači na škodlivý software a další potenciální hrozby.

Tuto kontrolu můžete také spustit kliknutím na **Volitelná kontrola** a vybráním možnosti **Výměnné disky** z rozbalovacího menu **Cíle kontroly**.

Opakovat poslední kontrolu

Pomocí této možnosti spustí znovu naposledy prováděnou kontrolu se stejnými cíli i parametry.

Pomocí rozbalovacího menu **Akce po kontrole** můžete nastavit akci (Žádná akce, Vypnout, Restartovat, Uspat), kterou chcete provést po dokončení kontroly.

Poznámka: Doporučujeme spouštět kontrolu počítače alespoň jednou za měsíc. Kontrolu je možné nastavit i jako naplánovanou úlohu pomocí **Nástroje** > **Další nástroje** > **Plánovač**.

4.1.1.2.1 Spuštění volitelné kontroly

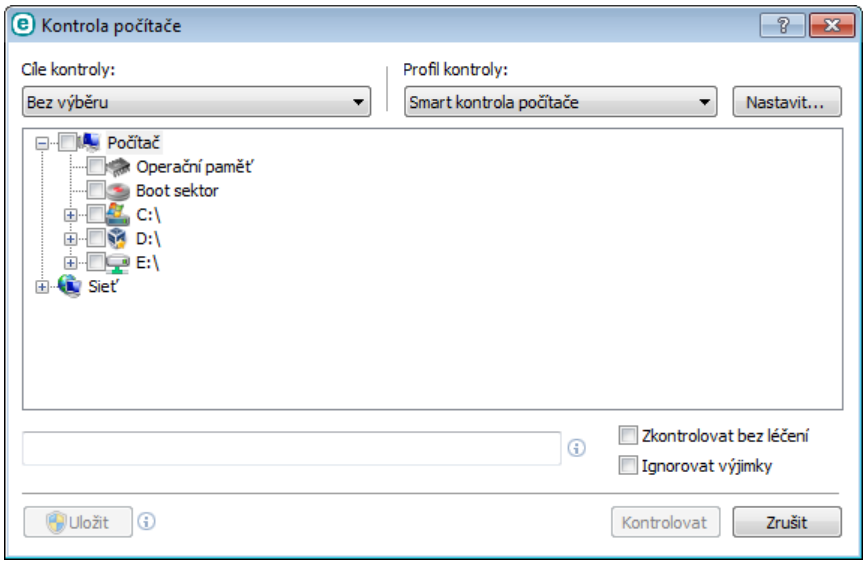
Pokud nechcete kontrolovat celý disk, ale pouze specifickou oblast, vyberte možnost Volitelná kontrola kliknutím v hlavním okně na záložku **Kontrola počítače** > **Volitelná kontrola** a ve stromové struktuře vyberte cíle kontroly.

Cíle kontroly slouží k výběru objektů (operační paměť, jednotky, sektory, soubory a složky), které mají být zkontrolovány. Cíl vyberte ve stromové struktuře, která zobrazuje seznam dostupných zařízení v počítači. Rozbalovací menu **Cíle kontroly** umožňuje vybrat ke kontrole předdefinované cíle**.**

- **Podle nastavení profilu** – vybere cíle uložené v profilu.
- **Výměnné disky** – vybere diskety, USB flash disky, CD/DVD.
- **Lokální disky** - vybere lokální pevné disky v počítači.
- **Síťové disky** – vybere namapované síťové disky.
- **Bez výběru** – zruší výběr cílů.

Prázdný řádek pod stromovou strukturou slouží pro rychlý přesun ke zvolenému cíli, nebo k přímému zadání

požadovaného cíle. Přímé zadání požadovaného cíle je možné pouze v případě, že není ve stromové struktuře proveden žádný výběr (v rozbalovacím menu **Cíle kontroly** je vybrána možnost **Bez výběru**).



Infikované soubory nejsou léčeny automaticky. Kontrolou bez léčení můžete získat přehled o aktuálním stavu bezpečnosti počítače. V případě, že máte zájem pouze o kontrolu souborů bez jejich následného léčení, zaškrtněte vpravo dole možnost **Kontrolovat bez léčení**. Kliknutím na **Nastavit** můžete následně na záložce **Parametry skenovacího jádra ThreatSense** pomocí rozbalovacího menu **Léčení** nastavit 3 úrovně léčení kontrolovaných souborů. Informace o provedené kontrole se uloží do protokolu.

Pro kontrolu můžete použít předdefinované profily v rozbalovacím menu **Profil kontroly**. Standardním profilem je **Smart kontrola** počítače. Dále jsou dostupné dva předdefinované profily pojmenované **Hloubková kontrola počítače** a **Kontrola počítače z kontextového menu**. Navzájem se liší odlišným nastavením parametrů skenovacího jádra ThreatSense. Kliknutím na tlačítko **Nastavit...** zobrazíte podrobné nastavení. Dostupné možnosti v sekci **Ostatní** jsou popsány v kapitole nastavení parametrů skenovacího jádra ThreatSense.

Kliknutím na tlačítko **Uložit** uložíte změny provedené v nastavení kontroly, včetně výběru ve stromové struktuře.

Kliknutím na tlačítko **Kontrolovat** spustíte kontrolu počítače s nastavenými parametry.

Kliknutím na tlačítko **Kontrolovat jako Administrátor** spustíte kontrolu po účtem Administrátora. Tuto funkci použijte v případě, že aktuálně přihlášený uživatel nemá dostatečná práva pro kontrolu složek. Mějte na paměti, že tlačítko není dostupné, pokud uživatel nemůže provádět UAC operace jako administrátor.

4.1.1.2.2 Průběh kontroly

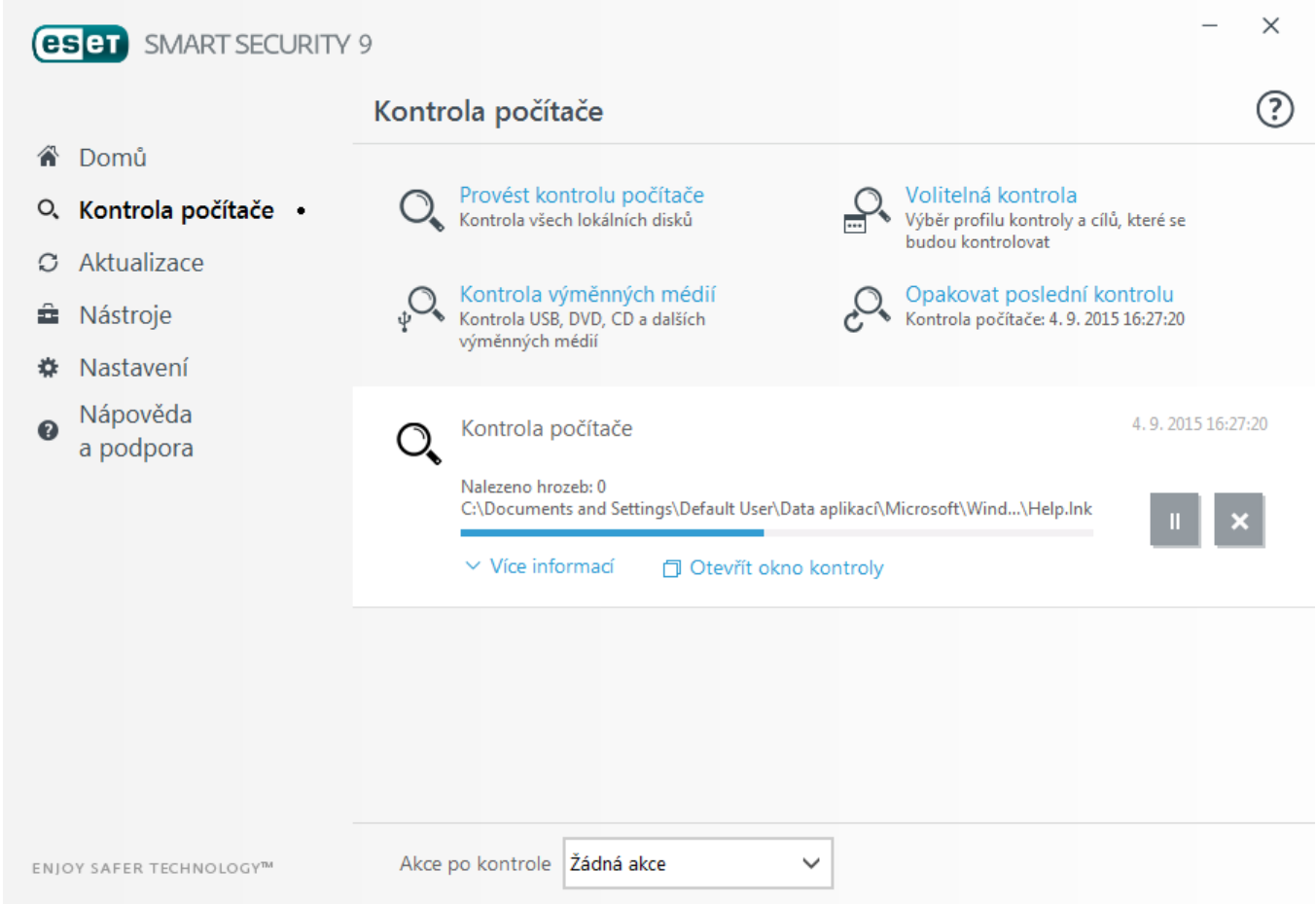
Okno průběhu kontroly zobrazuje aktuální stav kontroly a počet souborů, které obsahují škodlivý kód.

Poznámka: Je v pořádku, pokud určité typy souborů jako například zaheslovaná data nebo soubory využívané operačním systémem (například *pagefile.sys* a některé soubory protokolů) nemohou být zkontrolovány.

Průběh kontroly – grafická reprezentace procentuálního vyjádření poměru již zkontrolovaných souborů k celkovému množství souborů, které se mají kontrolovat.
Cíl – název právě kontrolovaného souboru a jeho umístění.
Nalezeno hrozeb – celkový počet nalezených hrozeb v průběhu aktuální kontroly.
Pauza – pozastaví právě probíhající kontrolu.
Pokračovat – tato možnost se zobrazí po pozastavení kontroly. Kliknutím na toto tlačítko bude kontrola pokračovat.
Zastavit – přeruší právě probíhající kontrolu.
Rolovat výpis protokolu kontroly – pokud je tato možnost zapnuta, v dialogovém okně protokolu kontroly uvidíte vždy naposledy zkontrolované soubory.

TIP:

Pro zobrazení detailních informací klikněte na možnost **Více informací** nebo na **Otevřít okno kontroly**.
Kdykoli můžete spustit další kontrolu počítače. Mějte na paměti, že více souběžných kontrol může mít negativní dopad na výkon počítače.



Pomocí možnosti **Akce po kontrole** můžete nastavit akci (Žádná akce, Vypnout, Restartovat, Uspat), kterou chcete provést po dokončení kontroly. Dialog s informací o vypnutí počítače se zobrazí po dobu 1 minuty.

4.1.1.2.3 Profily kontroly

Oblíbená nastavení kontroly počítače si můžete uložit do profilů pro jejich opakované použití v budoucnu. Doporučujeme vytvořit několik profilů s různými cíli a metodami kontroly, případně s dalšími parametry.

Pro vytvoření nového profilu otevřete **Rozšířené nastavení** (dostupné po stisknutí klávesy F5 v hlavním okně programu), přejděte na záložku **Antivir** > **Volitelná kontrola počítače**. Kliknutím na **Změnit** na řádku **Profily** se zobrazí seznam existujících profilů kontroly počítače s možností vytvořit nový profil. V kapitole parametry skenovacího jádra ThreatSense naleznete popis jednotlivých parametrů pro nastavení kontroly počítače.

Příklad: Chcete vytvořit vlastní profil kontroly počítače a částečně vám vyhovuje nastavení předdefinovaného profilu **Smart kontrola počítače**, ale nechcete zároveň kontrolovat runtime archivy, potenciální nebezpečné aplikace a přitom požadujete **Přísné léčení**? Vytvořte nový profil kliknutím na tlačítko **Přidat** v Seznamu profilů Následně nově vytvořený profil vyberte z rozbalovacího menu **Aktivní profil** nastavte si parametry kontroly podle potřeby.

4.1.1.3 Kontrola po startu

Standardně se provádí během startu počítače a po aktualizaci virové databáze kontrola souborů zaváděných při startu počítače do operační paměti. Tato kontrola závisí na nastavení úloh v Plánovači.

Možnosti nastavení kontroly po startu jsou součástí naplánované úlohy **Kontrola souborů spouštěných po startu**. Pro změnu tohoto nastavení klikněte v hlavním okně na záložku **Nástroje** > **Plánovač** > **Kontrola souborů spouštěných po startu** a následně na tlačítko **Změnit**. V posledním kroku se zobrazí okno Kontrola souborů spouštěných po startu počítače (pro více informací přejděte do další kapitoly).

Více informací o tvorbě a správě úloh Plánovače naleznete v kapitole Vytvoření nové úlohy.

4.1.1.3.1 Kontrola souborů spouštěných při startu počítače

Při vytvoření naplánované úlohy zajišťující kontroly souborů spouštěných při startu operačního systému můžete vybírat z níže uvedených parametrů.

Rozbalovací menu **Hloubka kontroly** nabízí možnost přizpůsobit množství souborů kontrolovaných při startu. Možnosti kontroly jsou seřazeny vzestupně podle následujících kritérií:

- **Pouze nejčastěji používané soubory** (nejméně kontrolovaných souborů),
- **Často používané soubory**,
- **Běžně používané soubory**,
- **Málo používané soubory**,
- **Všechny registrované soubory** (nejvíce kontrolovaných souborů).

Mezi tyto možnosti patří také tyto dvě:

- **Soubory spouštěné před přihlášením uživatele** – zahrnuje soubory z míst, ke kterým může být přistupováno bez toho, aby byl uživatel přihlášen (typicky všechny položky po spuštění jako jsou služby, browser helper objects, winlogon oznámení, záznamy plánovače Windows, známé dll atd.),
- **Soubory spouštěné po přihlášení uživatele** – zahrnuje soubory z míst, ke kterým může být přistupováno až po přihlášení uživatele (typicky soubory, které jsou spouštěny pro daného uživatele, nejčastěji umístěné v klíči registru *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Seznamy souborů ke kontrole jsou pro každou skupinu pevně definovány.

Priorita kontroly – umožňuje nastavit úroveň priority, při které se spustí kontrola počítače:

- **Normální** – zatížení systému je normální,
- **Nižší** – zatížení systému je nižší,
- **Nejnižší** – zatížení systému je nejnižší,
- **Při nečinnosti** – v momentě, kdy nejsou prováděny žádné jiné činnosti.

4.1.1.4 Kontrola při nečinnosti

Kontrolu při nečinnosti můžete nastavit v **Rozšířeném nastavení** na záložce **Antivir** > **Kontrola v nečinnosti** > **Obecné**. Funkci aktivujete pomocí přepínače **Zapnout kontrolu při nečinnosti**. Tichá kontrola všech lokálních disků v počítači se spouští v případě, že je počítač ve stavu nečinnosti. Více informací o možnostech definování akce, při které se spustí kontrola naleznete v kapitole Detekce nečinnosti.

Standardně se kontrola při nečinnosti nespouští, pokud je počítač (notebook) napájen z baterie. Toto nastavení můžete změnit zaškrtnutím možnosti **Spustit také při napájení počítače z baterie** v Rozšířeném nastavení.

Vyberte možnost **Zapisovat do protokolu**, pokud chcete průběh kontroly zapisovat do protokolu a mít k výsledkům přístup ze sekce **Nástroje** > **Protokoly**, kde z rozbalovacího menu vyberete možnost **Kontrola počítače.**

Kontrola při nečinnosti se může spustit při těchto událostech:

- Spuštění spořiče obrazovky,
- Uzamčení počítače,
- Odhlášení obrazovky.

Pro úpravu parametrů prováděné kontroly (například režimu detekce, úrovně léčení atp.) přejděte do sekce parametry skenovacího jádra ThreatSense.

4.1.1.5 Výjimky

Výjimky umožňují definovat soubory a složky, které nemají být kontrolovány. Pro zajištění kontroly všech objektů na hrozby doporučujeme výjimky vytvářet pouze v nevyhnutelných případech. Přesto někdy mohou nastat situace, kdy je nutné objekt vyloučit z kontroly, například u velkých databází, jejichž kontrola by zpomalila počítač nebo aplikací, u kterých dochází ke konfliktu se skenovacím jádrem.

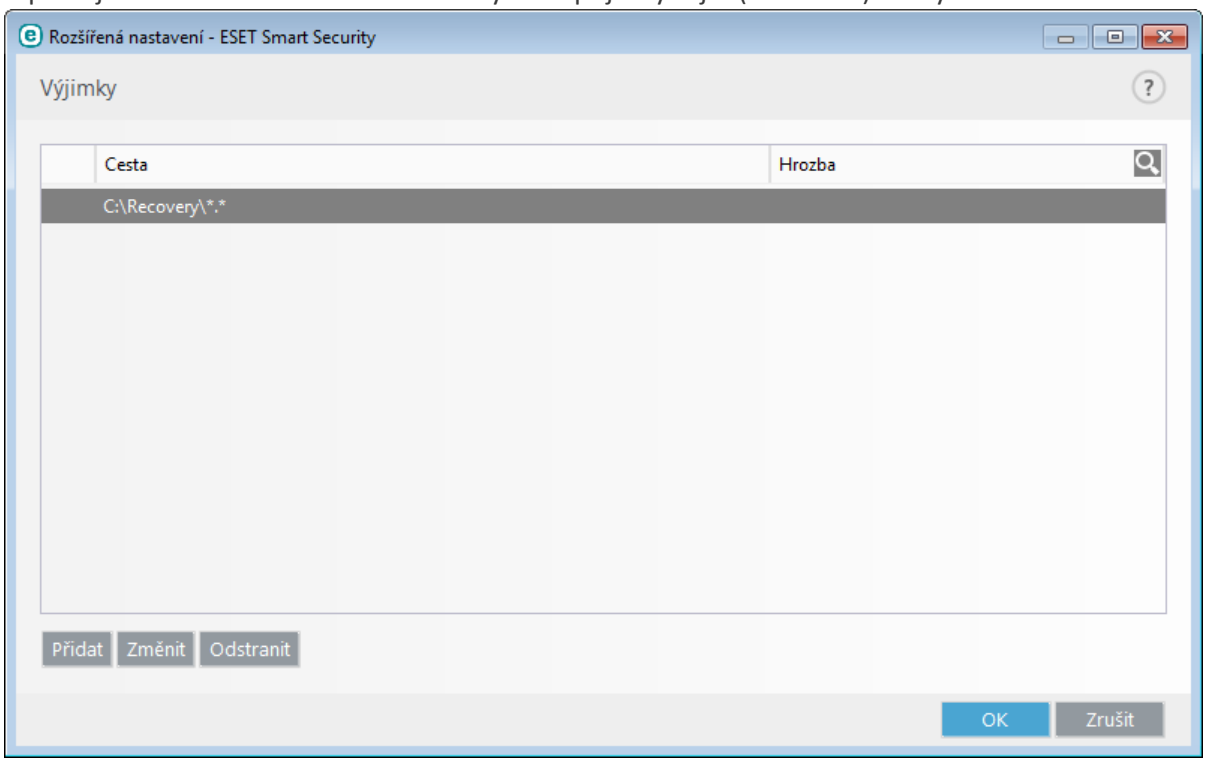
Pro vyloučení objektu z kontroly:

- Klikněte na **Přidat** a zadejte cestu k objektu nebo ji vyberte ručně ze stromové struktury.

Pro vyloučení skupiny souborů z kontroly můžete použít zástupné znaky. Otazník (?) reprezentuje jeden znak zatímco hvězdička (*) reprezentuje celý řetězec znaků.

Příklady

- Pokud chcete vyloučit ve vybrané složce všechny soubory, zadejte cestu ke složce a použijte masku "*.*".
- Pro vyloučení celé jednotky včetně všech souborů a složek použijte masku "D:*".
- Pokud chcete vyloučit všechny .doc soubory, použijte masku "*.doc".
- Pokud se název spustitelného souboru skládá z určitého počtu znaků, ale nevíte jakých, přesto znáte počáteční, použijte formát "D????. exe". Otazníky zastupují chybějící (neznámé) znaky.



Poznámka: Soubory zařazené do výjimek nebudou kontrolovány rezidentní ochranou ani naplánovanou nebo ručně spuštěnou kontrolou počítače, i když budou napadeny škodlivým kódem.

Sloupce

Cesta – cesta k vyloučenému souboru nebo složce.

Hrozba – pokud je u vyloučeného souboru uveden i název infiltrace, znamená to, že u souboru je vyloučena pouze detekce této infiltrace. Není však vyloučen soubor jako celek. Pokud by tedy došlo k napadení takto vyloučeného souboru jinou infiltrací, ta bude antivirovým modulem řádně detekována. Tento typ vyloučení je možné použít pouze pro určité typy infiltrací a zadat je můžete pomocí zobrazeného dialogového okna při výskytu hrozby (po kliknutí na **Zobrazit rozšířené nastavení** > **Vyloučit z detekce**), nebo prostřednictvím možnosti **Obnovit a vyloučit z kontroly** z kontextového menu po kliknutí pravým tlačítkem myši na soubor v karanténě.

Ovládací prvky

Přidat – přidá objekt na seznam výjimek.

Změnit – upraví existující výjimku.

Odstranit – odstraní výjimku.

4.1.1.6 Parametry skenovacího jádra ThreatSense

ThreatSense je název technologie, kterou tvoří soubor komplexních metod detekce infiltrace. Tato technologie je proaktivní a poskytuje tak ochranu i během prvních hodin šíření nové hrozby. K odhalení hrozeb využívá kombinaci několika metod (analýza kódu, emulace kódu, generické signatury, virové signatury), čímž efektivně spojuje jejich výhody. Detekční jádro je schopné kontrolovat několik datových toků paralelně a maximalizovat tak svůj výkon a účinnost detekce. Technologie ThreatSense dokáže účinně bojovat také s rootkity.

Ve skenovacím jádru ThreatSense můžete definovat následující parametry:

- Typu souborů a přípon, které se mají kontrolovat,
- Kombinace různých metod detekce,
- Úrovně léčení apod.

Pro zobrazení nastavení klikněte na záložku **Parametry skenovacího jádra ThreatSense** v Rozšířeném nastavení jakéhokoli modulu, který používá ThreatSense technologii (viz níže). Pro různé druhy ochrany se používá různá úroveň nastavení. ThreatSense je možné konfigurovat individuálně pro následující moduly:

- Rezidentní ochrana souborového systému,
- Ochrana dokumentů,
- Ochrana poštovních klientů,
- Ochrana přístupu na web,
- Kontrola počítače.

Parametry ThreatSense jsou optimalizovány speciálně pro každý modul a jejich změna může mít výrazný dopad na výkon systému. Příkladem může být zpomalení systému při povolení kontroly runtime archivů a rozšířené heuristiky pro rezidentní ochranu souborů (standardně jsou kontrolovány pouze nově vytvářené soubory). Proto doporučujeme ponechat původní nastavení ThreatSense pro všechny druhy ochran kromě **Kontroly počítače**.

Kontrolované objekty

V této sekci můžete vybrat součásti počítače a soubory, které budou testovány na přítomnost infiltrace.

Operační paměť – kontrola přítomnosti hrozeb, které mohou být zavedeny v operační paměti počítače.

Boot sektory – kontrola přítomnosti boot virů v MBR sektorech disků, kde se nachází tzv. zavaděč operačního systému.

Poštovní soubory – podporovány jsou DBX (Outlook Express) a EML soubory.

Archivy – podporovány jsou formáty ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO, BIN, NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE a jiné.

Samorozbalovací archivy – archivy které nepotřebují pro své rozbalení jiné programy. Jedná se o SFX (Self-extracting) archivy.

Runtime archivy – runtime archivy se na rozdíl od klasických archivů po spuštění rozbalí v paměti počítače. Kromě podpory tradičních statických archivátorů (UPX, yoda, ASPack, FSG,...) program podporuje díky emulaci kódu i mnoho jiných typů archivátorů.

Možnosti kontroly

V sekci **Možnosti kontroly** můžete vybrat metody, které se použijí pro ověřování přítomnosti infiltrace. Dostupné jsou následující možnosti:

Heuristika – heuristika je algoritmus, který analyzuje (nežádoucí) aktivity programů. Výhodou heuristiky je schopnost odhalit i takový škodlivý software, který v době poslední aktualizace antivirového programu ještě neexistoval nebo nebyl znám. Nevýhodou je nízká pravděpodobnost falešného poplachu.

Rozšířená heuristika/DNA/Smart vzorky – rozšířená heuristika se skládá z unikátních heuristických algoritmů vyvinutých společností ESET optimalizovaných pro detekci škodlivých kódů napsaných ve vyšších programovacích jazycích. Používání rozšířené heuristiky výrazně zvyšuje detekční schopni produktů ESET. Vzorky zajišťují přesnou

detekci virů. S využitím automatického aktualizačního systému mají nové vzorky uživatelé k dispozici do několika hodin od objevení hrozby. Nevýhodou vzorků je detekce pouze známých virů.

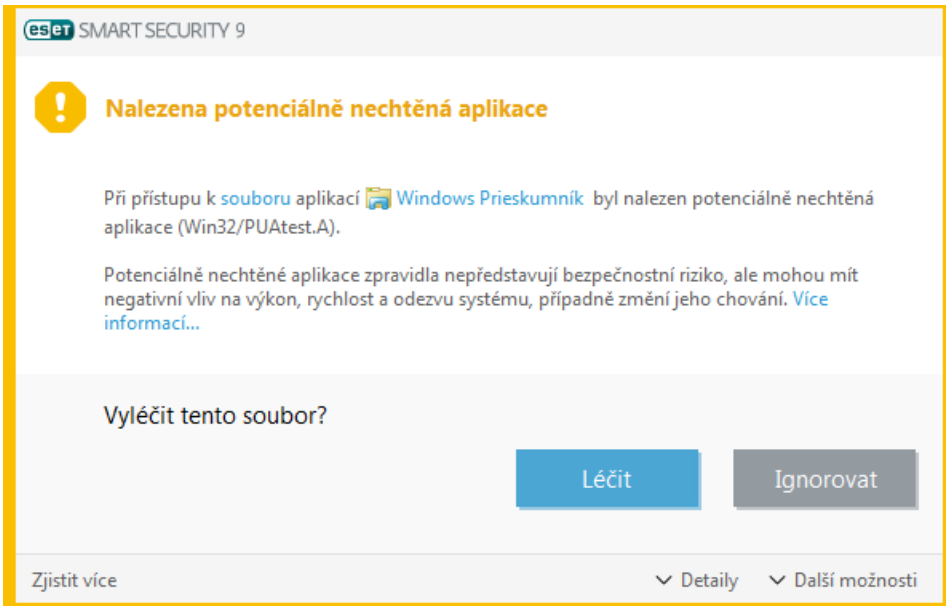
Potenciálně nechtěné aplikace jsou programy, které sice nemusí představovat bezpečnostní riziko, ale mohou mít negativní dopad na výkon počítače. Tyto aplikace se obvykle do systému nainstalují až po souhlasu uživatele. Jejich instalací dojde k určitým změnám v chování počítačového systému oproti stavu bez instalace příslušné aplikace. Mezi tyto změny v systému patří zejména:

- zobrazování oken (pop-up, reklamy), které by se jinak nezobrazovaly,
- aktivace a spuštění skrytých procesů,
- zvýšená spotřeba systémových prostředků,
- změny výsledků vyhledávání,
- komunikace se servery výrobce aplikace.

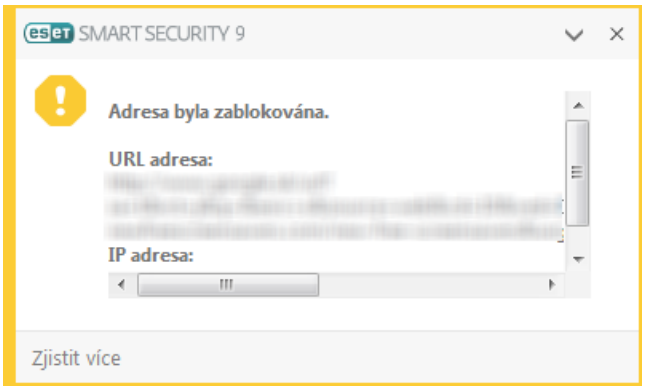
Varování - Nalezena potenciální hrozba

Při detekování potenciálně nechtěné aplikace se zobrazí dialogové okno s možností výběru akce:

1. **Vyléčit/Odpojit** – vybráním této možnosti zabráníte spuštění nebo stažení aplikace, a zabráníte tak infiltraci systému.
2. **Žádná akce** – po vybrání této možnosti se do vašeho systému dostane potenciální hrozba.
3. Pokud chcete danou aplikaci používat a nechcete aby vás produkt ESET upozorňoval na potenciální riziko, klikněte na **Zobrazit možnosti** a zaškrtněte možnost **Vyloučit z detekce**.

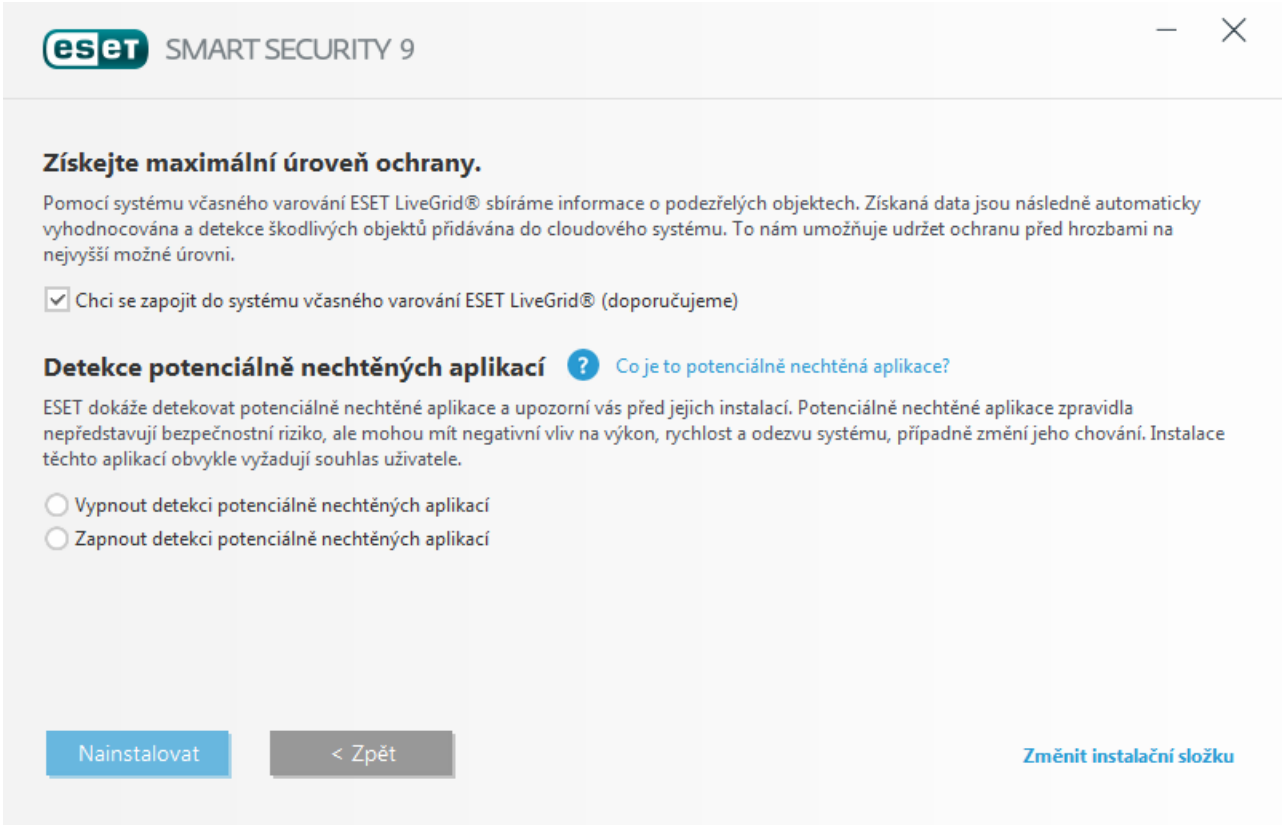


Pokud bude detekována potenciálně nechtěná aplikace a není možné ji vyléčit, při komunikaci dané aplikace se vzdálenou stranou se zobrazí upozornění **Adresa byla zablokována**. Zároveň se tato informace zapíše do protokolu a více informací naleznete v hlavním menu programu na záložce **Nástroje** > **Další nástroje** > **Protokoly** > **Filtrované webové stránky**.



Potenciálně nechtěné aplikace – Nastavení

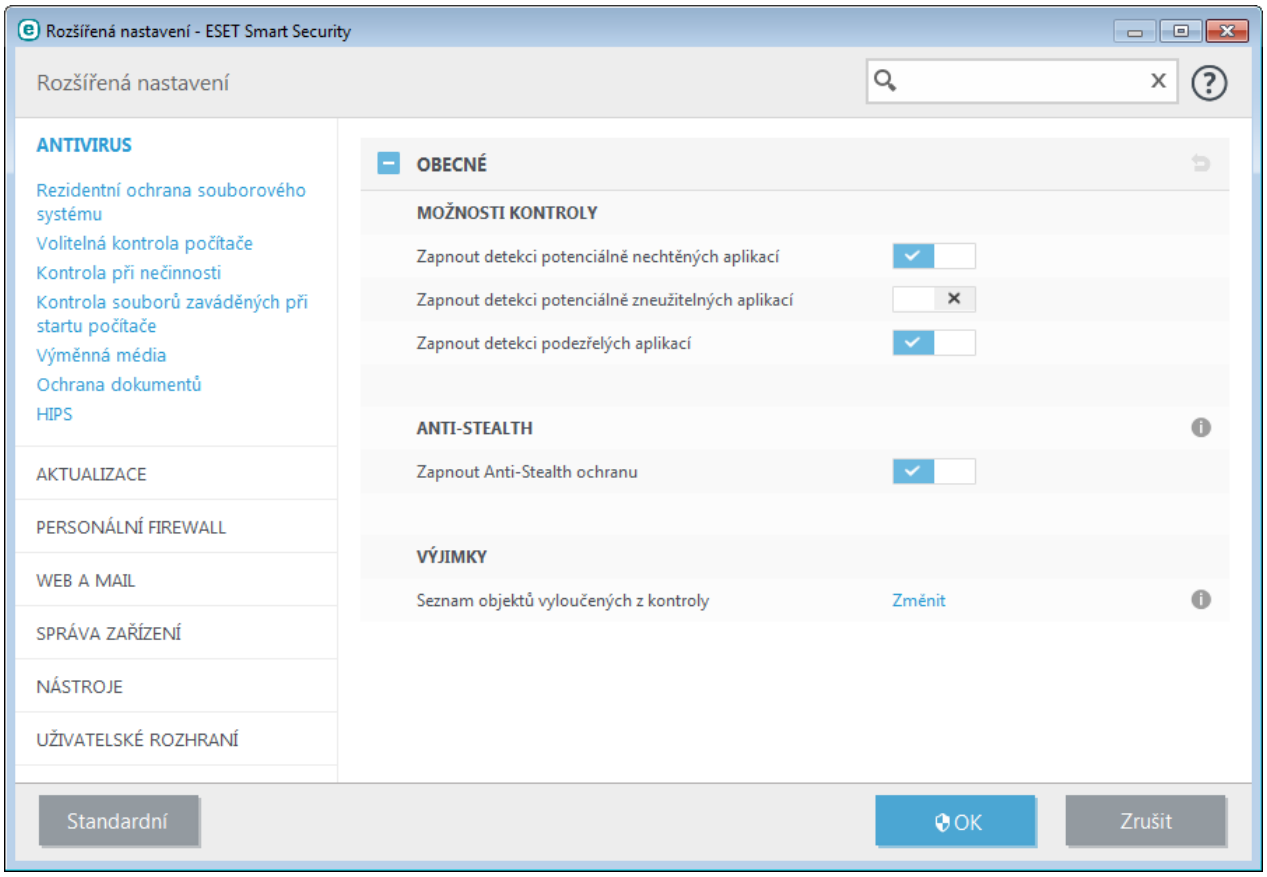
Již při instalaci produktu ESET se můžete rozhodnout, zda chcete být upozorňováni na potenciálně nechtěné aplikace:



Potenciálně nechtěné aplikace mohou do vašeho systému doinstalovat adware, toolbary nebo další aplikace, které mohou ve vašem systému provádět nechtěné a nebezpečné operace.

Nastavení detekce těchto aplikací můžete kdykoli změnit v nastavení programu. Pro úpravu detekce postupujte podle následujících kroků:

1. Otevřete hlavní okno produktu ESET. Pokud nevíte jak, postupujte podle tohoto návodu.
2. Stiskněte klávesu F5 a zobrazte **Rozšířená nastavení**.
3. Přejděte na záložku **Antivirus**, kde jsou dostupné následující možnosti: **Zapnout detekci potenciálně nechtěných aplikací**, **Zapnout detekci potenciálně zneužitelných aplikací** a **Zapnout detekci podezřelých aplikací**. Pro uložení změn klikněte na tlačítko **OK**.



Potenciálně nechtěné aplikace – Software wrappery

Software wrapper představuje speciální typ úpravy aplikace, který používají některé softwarové portály. Vámi požadovanou aplikaci nestahujete napřímo, ale prostřednictvím nástroje třetí strany. Tyto nástroje kromě požadované aplikace do systému instalují adware nebo toolbary. Kromě originální aplikace se mohou tyto nástroje, které dále mohou měnit domovskou stránku ve vašem prohlížeči a ovlivňovat výsledky vyhledávání. Protože softwarové portály v drtivé většině neinformují koncového uživatele, že ke stažení aplikace dojde prostřednictvím nástroje třetí strany, společnost ESET detekuje tzv. software wrappery jako potenciálně nechtěné aplikace. V takovém případě máte na výběr, zda chcete pokračovat ve stahování nebo si najít jiný zdroj.

Nejnovější verzi této kapitoly naleznete v ESET Databázi znalostí.

Potenciálně zneužitelné aplikace – Potenciálně zneužitelné aplikace jsou komerční a legitimní aplikace například pro zobrazení vzdálené pracovní plochy, dešifrování kódů a hesel nebo tzv. keyloggery (programy na monitorování stisknutých kláves). Detekce těchto aplikací je standardně vypnuta.

ESET LiveGrid® – prostřednictvím této reputační technologie jsou kontrolované soubory ověřovány vůči cloudového systému ESET LiveGrid® s cílem dosažení přesnější detekce a zrychlení kontroly.

Léčení

Nastavení léčení ovlivňuje chování virové skeneru. K dispozici jsou 3 úrovně léčení detekovaných infikovaných souborů:

Neléčit – infikované soubory nebudou automaticky léčeny. Při detekci se zobrazí varovné okno s možností výběru akce, která se má provést. Tato úroveň je navržena pro pokročilé uživatele, kteří vědí, jak postupovat v případě infiltrace.

Standardní úroveň léčení – program se pokusí infikované soubory automaticky léčit, nebo odstranit na základě předdefinované akce (v závislosti na typu infiltrace). Informace o detekci a odstranění infikovaného souboru je zobrazena informační bublinou v pravém dolním rohu obrazovky. Pokud program nedokáže automaticky vybrat správnou akci, zobrazí se okno s možností výběru akce. Možnost výběru akce se zobrazí také v případě, když se předdefinovanou akci nepodaří provést.

Přísné léčení – program vyléčí nebo odstraní všechny infikované soubory. Výjimku tvoří systémové soubory. Pokud

je nelze vyléčit, zobrazí se výběr akce, která se má provést.

Varování: Při detekci infiltrace v archivu, bude při standardním a přísném léčení odstraněn celý archiv. Při standardním léčení bude archiv odstraněn, pouze pokud obsahuje samotný soubor s infiltrací. Při **přísném léčení** bude archiv odstraněn i v případě, že kromě infiltrace obsahuje další korektní soubory.

Výjimky

Přípona je část názvu souboru oddělená tečkou. Přípona určuje typ a obsah souboru (například *dokument.txt* označuje textový dokument). V této části nastavení ThreatSense nastavíte typy souborů, které chcete vyloučit z kontroly.

Ostatní

Při konfiguraci parametrů skenovacího jádra ThreatSense jsou v sekci **Ostatní** k dispozici následující možnosti:

Kontrolovat alternativní datové proudy (ADS) – alternativní datové proudy (ADS) používané systémem NTFS jsou běžným způsobem neviditelné asociace k souborům a složkám. Mnoho virů je proto využívá jako maskování před případným odhalením.

Spustit kontrolu na pozadí s nízkou prioritou – každá kontrola počítače využívá určité množství systémových zdrojů. Pokud právě pracujete s programy náročnými na výkon procesoru, přesunutím kontroly na pozadí jí můžete přiřadit nižší prioritu a získat více prostředků pro ostatní aplikace.

Zapisovat všechny objekty do protokolu – pokud je tato možnost aktivní, do protokolu se zapíší všechny zkontrolované soubory, i když nejsou infikované. Například, při nalezení infiltrace v archivu, se do protokolu zapíší všechny soubory z archivu, i když jsou čisté.

Používat Smart optimalizaci – při zapnuté Smart optimalizaci je použito nejoptimálnější nastavení pro zajištění maximální efektivity kontroly při současném zachování vysoké rychlosti. Každý modul ochrany kontroluje objekty inteligentně a používá odlišné metody, které aplikuje na specifické typy souborů. Pokud je Smart optimalizace vypnuta, použije se pouze uživatelské nastavení jádra ThreatSense.

Zachovat čas přístupu k souborům – při kontrole souboru nebude změněn čas přístupu, ale bude ponechán původní (vhodné při používání na zálohovacích systémech).

Omezení

V sekci **Omezení** můžete nastavit maximální velikost objektů, archivů a úroveň zanoření, které se budou testovat na přítomnost škodlivého kódu:

Nastavení objektů

Maximální velikost objektu – umožňuje definovat maximální hodnotu velikosti objektu, který bude kontrolován. Daný modul antiviru bude kontrolovat pouze objekty s menší velikostí než je definovaná hodnota. Tyto hodnoty doporučujeme měnit pouze pokročilým uživatelům, kteří chtějí velké objekty vyloučit z kontroly. Standardní hodnota: *neomezeno*.

Maximální čas kontroly objektu (v sekundách) – definuje maximální povolený čas na kontrolu objektu. Pokud nastavíte určitou hodnotu, po překročení této hodnoty skončí probíhající antivirová kontrola objektu bez ohledu na to, zda byla dokončena. Objekt může zůstat nezkontrolován. Standardní hodnota: *neomezeno*.

Nastavení archivů

Úroveň vnoření archivů – specifikuje maximální úroveň vnoření do archivu při antivirové kontrole. Standardní hodnota: *10*.

Maximální velikost souboru v archivu – specifikuje maximální velikost rozbaleného souboru v archivu, který je kontrolován. Standardní hodnota: *neomezeno*.

Poznámka: Antivirus standardně používá předdefinované hodnoty, které doporučujeme měnit pouze ve zvláštních případech.

4.1.1.6.1 Léčení

Nastavení léčení ovlivňuje chování virové skeneru. K dispozici jsou 3 úrovně léčení detekovaných infikovaných souborů.

4.1.1.6.2 Výjimky

Přípona je část názvu souboru oddělená tečkou. Přípona určuje typ a obsah souboru (například *dokument.txt* označuje textový dokument). V této části nastavení ThreatSense nastavíte, které typy souborů budou kontrolovány.

Standardně jsou kontrolovány všechny soubory bez ohledu na jejich příponu. Do seznamu souborů vyloučených z kontroly můžete přidávat libovolné přípony.

Definování výjimek je však doporučeno pouze v případě problémů s určitým programem, který dané typy souborů používá (například .edb, .eml a .tmp pro MS Exchange Server).

Pomocí tlačítka **Přidat** a **Odstranit** můžete povolit nebo zakázat kontrolování vybraných přípon souborů. Pro přidání přípony klikněte na tlačítko **Přidat**, do zobrazeného prázdného pole zadejte příponu a akci potvrďte kliknutím na tlačítko **OK**. Zadat můžete více hodnot oddělené čárkou, středníkem nebo zadejte každou příponu na nový řádek. Vybráním přípony v seznamu a kliknutím na tlačítko **Odstranit** příponu odstraníte ze seznamu. Pro úpravu přípony ji v seznamu vyberte a klikněte na tlačítko **Změnit**.

Pro definování seznamu výjimek můžete používat ? (otazník). Otazník (?) reprezentuje jeden znak.

Poznámka: Pro zobrazení přípony konkrétního souboru si zobrazte detailní informace o souboru (z kontextového menu vyberte možnost **Vlastnosti**) nebo si deaktivujte možnost **Skrýt přípony souborů známých typů** přímo v Průzkumníku Windows (**Ovládací panely** > **Možnosti složky** > **Zobrazení**).

4.1.1.7 Nalezena hrozba

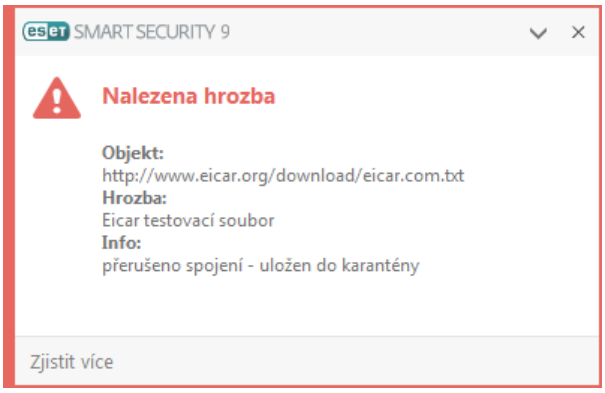
Infiltrace se mohou do počítače dostat z různých zdrojů: z webových stránek, ze sdílených složek, prostřednictvím e-mailu, z výměnných médií (USB klíče, externí disky, CD a DVD, diskety a jiné).

Standardní chování

ESET Smart Security dokáže zachytit infiltrace pomocí:

- Rezidentní ochrany souborového systému,
- Ochrany přístupu na web,
- Ochrany poštovních klientů,
- Kontroly počítače.

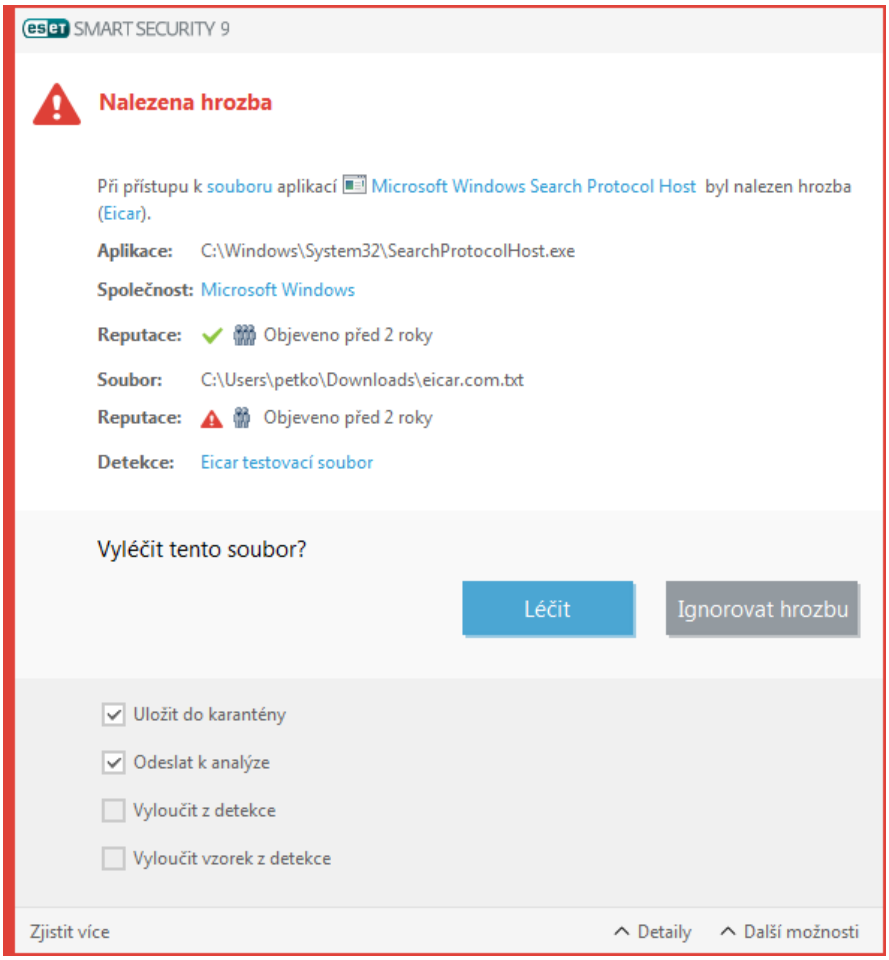
Každý z těchto modulů používá standardní úroveň léčení. Program se pokusí soubor vyléčit a přesunout do Karantény, nebo přeruší spojení. Oznámení se zobrazují v pravé dolní části obrazovky. Pro více informací o jednotlivých úrovních léčení a jejich chování si prosím přečtěte kapitolu Léčení.



Léčení a mazání

Pokud rezidentní ochrana nemá předdefinovanou akci pro daný typ souboru zobrazí se dialogové okno s výběrem akce. Obvykle jsou dostupné možnosti **Léčit**, **Vymazat** a **Žádná akce**. Výběr možnosti **Žádná akce** nedoporučujeme,

protože v tomto případě zůstane infekce nevyléčena. Výjimku tvoří případy, kdy jste si jisti, že je soubor neškodný a byl detekován chybně.



Léčení souboru je možné provést, pokud do zdravého souboru byla zavedena část, která obsahuje škodlivý kód. V tomto případě má smysl pokusit se infikovaný soubor léčit a získat tak původní zdravý soubor. V případě, že infiltrací je soubor, který obsahuje výlučně škodlivý kód, bude odstraněn.

Pokud je soubor uzamčen nebo používán systémovým procesem, bude obvykle odstraněn až po svém uvolnění, typicky po restartu počítače.

Více hrozeb

Pokud infikované soubory nebyly vymazány během kontroly počítače (nebo je Úroveň léčení nastavena na **Neléčit**), zobrazí se dialogové okno s výběrem akce. Vyberte akci, kterou chcete provést (akce se nastavuje individuálně pro každý soubor ze seznamu) a klikněte na **Dokončit**.

Mazání souborů v archivech

Pokud je zjištěna infiltrace uvnitř archivu, bude archiv při standardní úrovni léčení odstraněn pouze v případě, že obsahuje pouze infikovaný soubor. Archiv nebude vymazán, pokud kromě infiltrace obsahuje také nezávadné soubory. Opatrnost je potřeba dodržovat při nastavení přísné úrovně léčení, kdy v tomto případě bude archiv vymazán, bez ohledu na to, zda jeho obsah tvoří také zdravé soubory.

Pokud se váš počítač chová podezřele nebo máte podezření, že je infikován (zamrzá, je pomalý atp.), postupujte podle následujících kroků:

- Otevřete ESET Smart Security a přejděte na záložku **Kontrola počítače.**
- Klikněte na **Smart kontrola** (bližší informace naleznete v kapitole Kontrola počítače).
- Po dokončení kontroly se zobrazí protokol, ve kterém je uveden počet zkontrolovaných, infikovaných a vyléčených souborů.

Pokud chcete zkontrolovat pouze vybranou část disku, klikněte na **Volitelná kontrola** a vyberte cíle, které chcete

ověřit na přítomnost virů.

4.1.1.8 Ochrana dokumentů

Modul ochrany dokumentů zajišťuje kontrolu dokumentů Microsoft Office před jejich otevřením a také kontroluje automaticky stahované soubory pomocí Internet Explorer, jako například prvky Microsoft ActiveX. Tento modul přidává další bezpečnostní vrstvu do rezidentní ochrany a může být deaktivován pro zvýšení výkonu systému, na kterých neotevíráte velké množství dokumentů Microsoft Office.

Možnost **Zapnout ochranu dokumentů** aktivuje systém ochrany dokumentů. Pokud chcete tuto možnost upravit, otevřete si **Rozšířené nastavení** (dostupné po stisknutí klávesy **F5**) a přejděte na záložku **Antivirus** > **Ochrana dokumentů**.

Tento modul pracuje pouze s aplikacemi, které podporují rozhraní Microsoft Antivirus API (například Microsoft Office 2000 nebo Microsoft Internet Explorer 5.0 a vyšší).

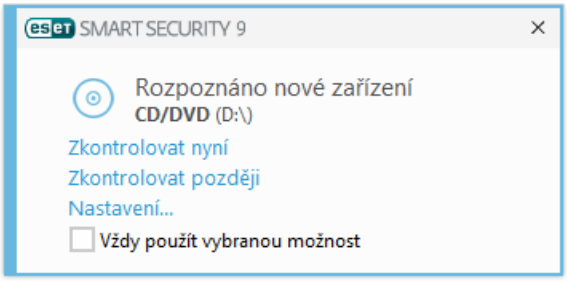
4.1.2 Výměnná média

ESET Smart Security poskytuje automatickou kontrolu výměnných médií (CD/DVD/USB/...). Tento modul umožňuje zkontrolovat obsah vložených médií. To může být užitečné v případě, kdy například administrátor potřebuje zajistit, aby uživatelé nevkládali výměnná média s nežádoucím obsahem do počítače.

Akce po vložení výměnného média – vyberte výchozí akci, kterou chcete provést při vložení výměnného média (CD/DVD/USB) do počítače. K dispozici jsou následující akce:

- **Nekontrolovat** – neprovede se žádná akce a nezobrazí se okno s možností výběru akce.
- **Automaticky zkontrolovat médium** – po vložení média se automaticky spustí volitelná kontra obsahu.
- **Zobrazit možnosti kontroly** – zobrazí uživateli okno s možností výběru akce.

Pokud vyberete **Zobrazit možnosti kontroly**, zobrazí se upozornění s výběrem akcí:



Zkontrolovat nyní – spustí se ruční kontrola výměnného média,

Zkontrolovat později – neprovede se žádná akce a okno Detekováno nové zařízení se zavře,

Nastavení... – otevře nastavení výměnných médií.

Kromě toho, ESET Smart Security disponuje pokročilými funkcemi pro správu zařízení, které vám umožňují definovat pravidla pro zacházení s externími zařízeními. Více informací naleznete v kapitole Správa zařízení.

4.1.3 Správa zařízení

ESET Smart Security poskytuje automatickou kontrolu výměnných médií (CD/DVD/USB/...). Tento modul umožňuje zkontrolovat obsah vložených médií. To může být užitečné v případě, kdy například administrátor potřebuje zajistit, aby uživatelé nevkládali výměnná média s nežádoucím obsahem do počítače.

Podporovaná externí zařízení:

- Datové úložiště (HDD, výměnné USB jednotky),
- CD/DVD,
- USB tiskárna,
- FireWire úložiště,
- Bluetooth zařízení,
- Čtečka čipových karet,
- Obrazové zařízení,
- Modem,
- LPT/COM port,
- Přenosné zařízení,
- Všechny typy zařízení.

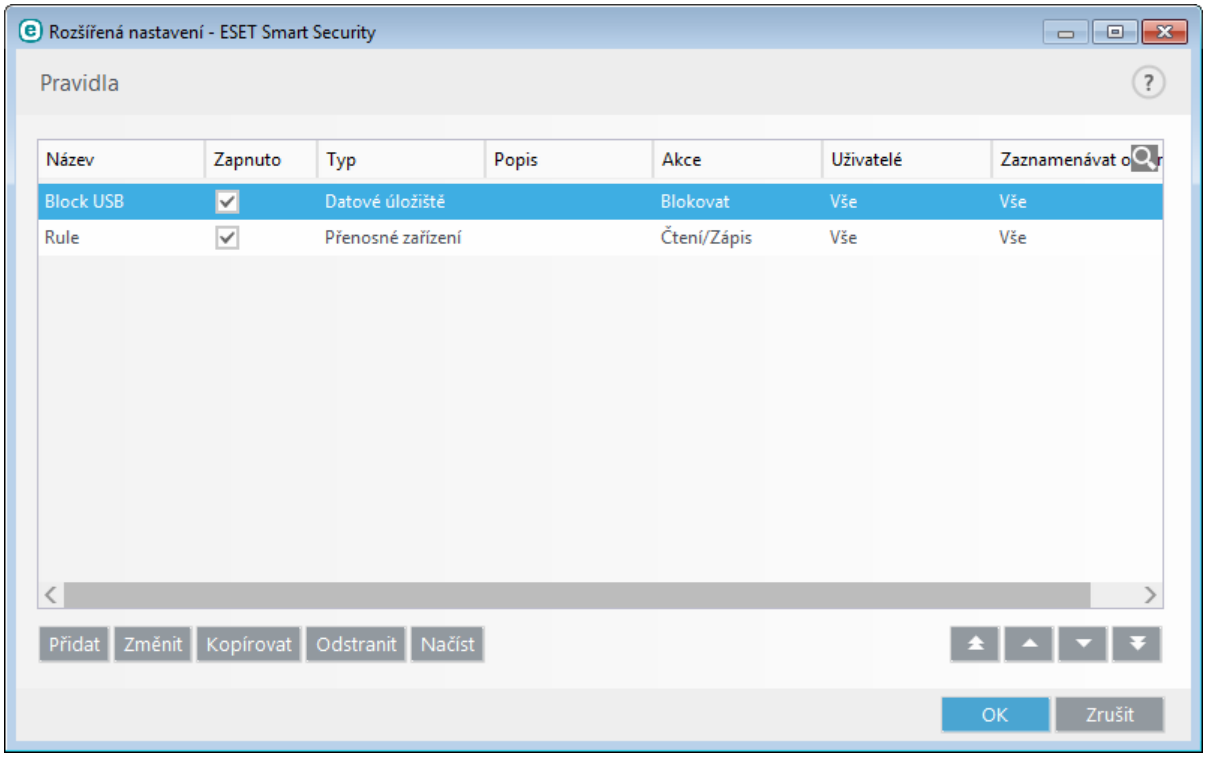
Nastavení Správce zařízení můžete upravit v **Rozšířeném nastavení** (dostupném po stisknutí **klávesy F5** v hlavním okně programu) > **Správa zařízení**.

Vybráním možnosti **Integrovat do systému** aktivujete funkci Správa zařízení programu ESET Smart Security. Pro provedení změn bude potřeba restartovat počítač. Po aktivaci této funkce bude dostupná možnost **Pravidla správy zařízení**, pomocí které si zobrazíte Editor pravidel správy zařízení.

Pokud do počítače vložíte externí zařízení, na které se použije pravidlo o blokování, zobrazí se v pravém dolním rohu obrazovky informační okno a přístup k zařízení bude zakázán.

4.1.3.1 Pravidla správy zařízení

Editor pravidel správy zařízení zobrazuje seznam všech existujících pravidel, které umožňují detailní kontrolu nad zařízeními připojovanými k počítači.



Konkrétní zařízení můžete povolit nebo zakázat pro vybraného uživatele nebo skupinu uživatelů na základě parametrů zařízení, které definujete v konfiguraci pravidla. Seznam pravidel obsahuje popis, tedy název pravidla, typ externích zařízení, akci, která se má provést po připojení k počítači a úroveň protokolování.

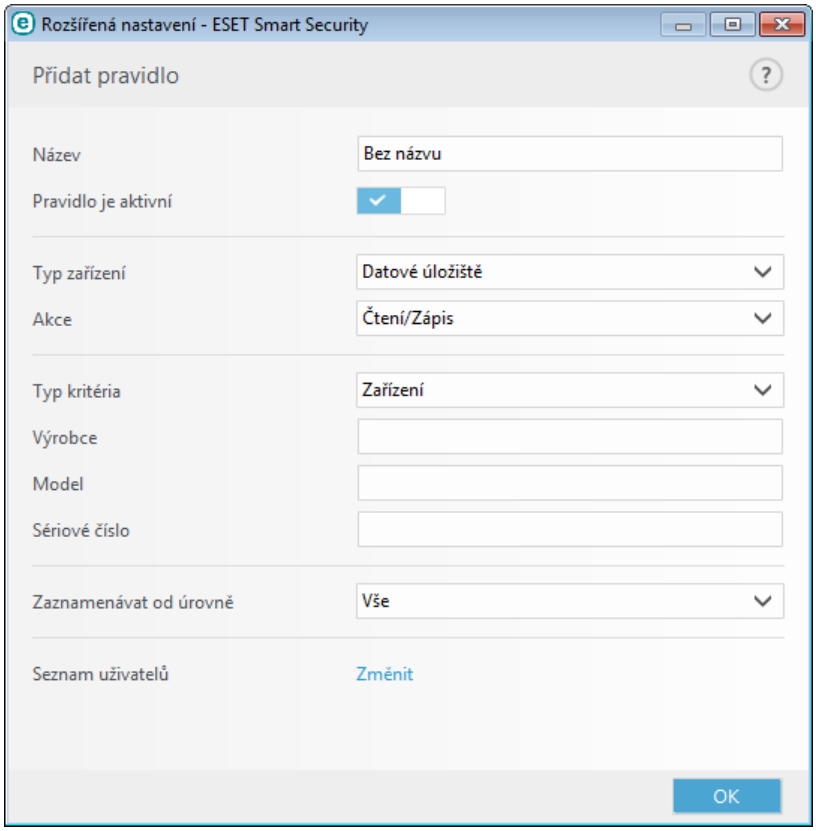
Pro správu pravidel klikněte na **Přidat** nebo **Změnit**. Stisknutím klávesy **CTRL** a kliknutím můžete vybrat více pravidel najednou a provést hromadné akce. Pomocí zaškrtávacího pole ve sloupci **Zapnuto** dané pravidlo zapnete nebo vypnete. To může být vhodné v případě, kdy nechcete pravidlo vymazat, ale ponechat si jej pro případné použití v budoucnu.

Pravidla jsou vyhodnocována na základě priority. Pravidlo s nejvyšší prioritou je umístěno v seznamu na prvním místě. Pravidla vztažená na URL mají vždy vyšší prioritu než pravidla vztažená na kategorii adres. Například, pravidlo na URL umístěné v seznamu níže, než pravidlo na kategorii, bude vyhodnoceno jako první.

Kliknutím na tlačítko **Načíst** se automaticky načtou parametry všech připojených výměnných zařízení připojených k počítači.

4.1.3.2 Vytvoření nového pravidla

V tomto okně můžete definovat akce, které se provedou po připojení daného zařízení k počítači.



Pro lepší přehlednost do pole **Název** zadejte jméno pravidla. Zaškrtnutím možnosti **Pravidlo je aktivní** dané pravidlo povolíte. Pokud ponecháte tuto možnost neaktivní, pravidlo se nebude uplatňovat a můžete jej použít v budoucnu.

Typ zařízení

Z rozbalovacího menu vyberte typ zařízení (diskové úložiště/přenosné zařízení/Bluetooth/FireWire/...). Typy zařízení se přebírají ze systému a můžete si je prohlídnout v systémovém Správci zařízení, který poskytuje informace o zařízeních připojených k počítači. Možnost Optická média představuje data uložená na optických médiích jako jsou CD nebo DVD. Úložná média zahrnuje externí disky nebo čtečky paměťových karet připojených pomocí USB nebo FireWire. Čtečky čipových karet zahrnují čtečky karet s integrovanými elektronickými obvody jako jsou SIM karty nebo přístupové karty. Příkladem zobrazovacích zařízení jsou fotoaparáty a kamery, které neposkytují informace o uživateli, pouze vyvolávají akce. To znamená, že tato zařízení mohou být blokována pouze globálně.

Akce

Přístup na zařízení, která neslouží pro ukládání dat, může být pouze povolen nebo zakázán. Oproti tomu úložným zařízením můžete nastavit následující práva:

- **Čtení/Zápis** – plný přístup k zařízení,
- **Blokovat** – přístup k zařízení bude zakázán,
- **Pouze pro čtení** – uživatel může pouze číst soubory na daném zařízení,

- **Upozornit** – při každém připojení zařízení se uživateli zobrazí upozornění, že byl přístup na zařízení povolen/zakázán a zároveň se informace zapíše do protokolu.

Mějte na paměti, že uvedené akce nemusí být dostupné u všech zařízení. Pokud se jedná o úložné zařízení, zobrazí se všechny. V případě zařízení, která neslouží pro ukládání dat, jsou dostupné pouze dvě akce (například akce **Pouze pro čtení** není dostupná pro Bluetooth zařízení, přístup k nim může být pouze povolen, zakázán).

Typ kritéria – vyberte, zda chcete pravidlo vytvořit pro jednotlivé zařízení nebo skupinu zařízení.

Pro přizpůsobení pravidel vztažených pouze na konkrétní zařízení můžete použít další parametry:

- **Výrobce** – filtruje podle názvu výrobce nebo ID,
- **Model** – filtruje podle názvu zařízení,
- **Sériové číslo** – filtruje podle sériového čísla, které zpravidla externí zařízení mají. V případě CD/DVD se jedná o sériové číslo média, nikoli mechaniky.

Poznámka: Pokud ponecháte výše uvedené údaje prázdné, pravidlo bude tyto hodnoty ignorovat. Filtrování parametrů rozlišuje velikost písmen a nepodporuje zástupné znaky (*, ?). Data musí být zadána tak, jak je poskytuje výrobce.

Tip: Pro získání parametrů zařízení, pro které chcete vytvořit pravidlo, připojte zařízení k počítači a ověřte detaily zařízení v Protokolu správy zařízení.

Zaznamenávat do protokolu

- **Vše** – zaznamenají se všechny události.
- **Diagnostické** – obsahují informace důležité pro ladění programu a všechny níže uvedené záznamy.
- **Informační** – obsahují informační zprávy, například o úspěšné aktualizaci a všechny níže uvedené záznamy.
- **Varování** – obsahují varovné zprávy a kritické chyby.
- **Žádné** – nebudou zaznamenávány žádné události nevytvoří se žádné protokoly.

Pravidla můžete přiřadit konkrétnímu uživateli nebo celé skupině uživatelů pomocí dialogového okna **Seznam uživatelů**.

- **Přidat** – otevře okno **Vybrat typ objektu: Uživatelé nebo Skupiny**, kde můžete vybrat konkrétní uživatele.
- **Vymazat** – odebere vybraného uživatele ze seznamu.

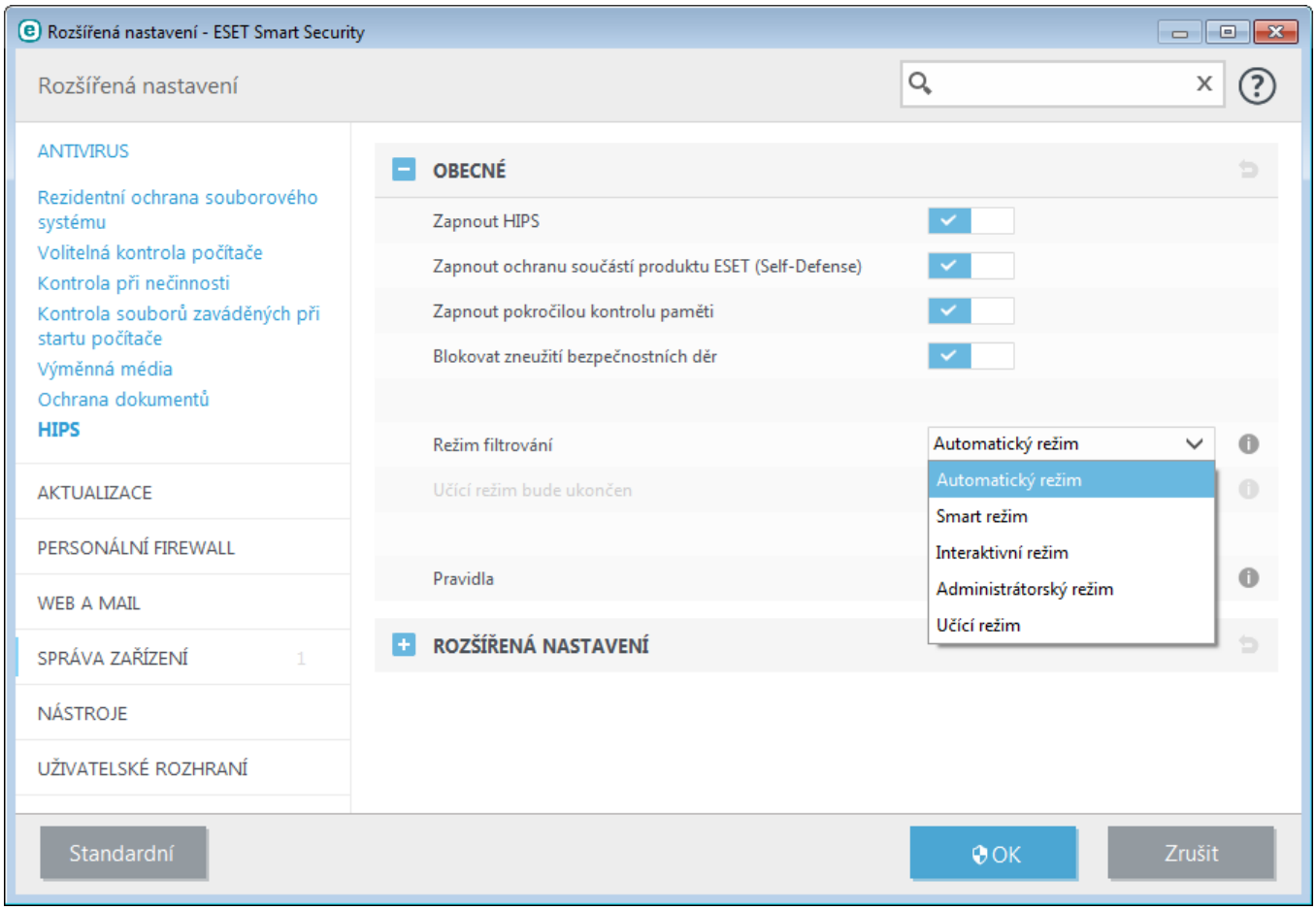
Mějte na paměti, že není možné omezit všechna zařízení. Například zobrazovací zařízení neposkytují žádné informace o uživateli, pouze vyvolávají akci.

4.1.4 HIPS


Pokud nejste zkušený uživatel, nedoporučujeme měnit nastavení systému HIPS. Chybnou úpravou nastavení HIPS se může systém stát nestabilní.

HIPS (Host-based Intrusion Prevention System) chrání operační systém před škodlivými kódy a eliminuje aktivity ohrožující bezpečnost počítače. HIPS používá pokročilou analýzu chování kódu, která spolu s detekčními schopnostmi síťového filtru zajišťuje efektivní kontrolu běžících procesů, souborů a záznamů v registru Windows. HIPS je nezávislý na rezidentní ochraně a firewallu a monitoruje pouze běžící procesy v operačním systému.

Nastavení HIPS naleznete v **Rozšířeném nastavení** (dostupném po stisknutí klávesy **F5**) na záložce **Antivirus** > **HIPS**. Stav ochrany HIPS je zobrazen v hlavním okně ESET Smart Security na záložce **Nastavení** v sekci **Počítač**.



ESET Smart Security má vestavěnou technologii *Self-Defense*, která brání škodlivé aplikaci v narušení nebo zablokování antivirové ochrany. *Self-Defense* chrání soubory a klíče v registru, které jsou kritické pro správnou funkci ESET Smart Security a neumožňuje potenciálnímu škodlivému software přístup k těmto záznamům a jejich úpravu. Změny nastavení provedete pomocí možnosti **Zapnout HIPS** a **Zapnout ochranu součástí produktu ESET (Self-Defense)** a projeví se až po restartu operačního systému. Z tohoto důvodu se také vypnutí celého systému **HIPS** projeví až po restartu počítače.

Pokročilá kontrola paměti v kombinaci s blokováním zneužití bezpečnostních děr poskytuje účinnou ochranu proti škodlivému kódu, který využívá obfuskaci a šifrování pro zabránění detekce. Tato funkce je standardně zapnuta. Pro více informací se podívejte do slovníku pojmů.

Blokování zneužití bezpečnostních děr (Exploit blocker) poskytuje další bezpečnostní vrstvu a chrání známé aplikace se zranitelnými bezpečnostními dírami (například webové prohlížeče, e-mailové klienty, pdf čtečky). Tato funkce je standardně zapnuta. Pro více informací se podívejte do slovník pojmů.

HIPS může běžet v jednom z následujících režimů:

Automatický režim s pravidly – operace budou povoleny s výjimkou předdefinovaných pravidel,

Interaktivní režim – uživatel bude na povolení či zakázání operace dotázán,

Administrátorský režim – operace jsou zablokované s výjimkou definovaných pravidel.

Smart režim – uživatel bude upozorněn pouze na podezřelé operace,

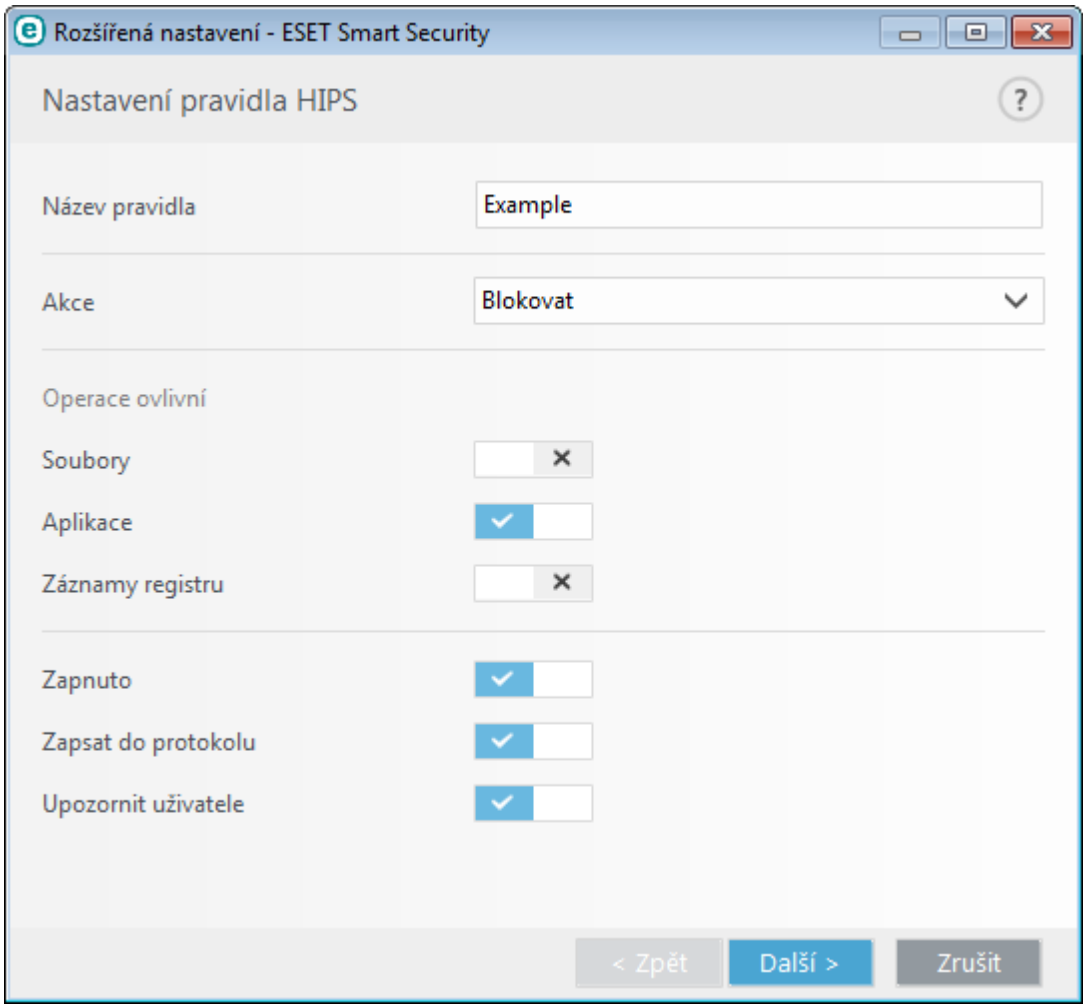
Učící režim – operace jsou povoleny a zároveň je vytvořeno pravidlo, které je povoluje. Pravidla vytvořená tímto režimem jsou viditelná v **Editoru pravidel**, ale mají nižší prioritu než pravidla vytvořená ručně nebo z dotazovacího dialogu v interaktivní režimu. Při zapnutém učícím režimu se zpřístupní možnost **Upozornit na ukončení učícího režimu za X dní.** Po této nastavené době se učící režim automaticky ukončí. Maximální počet dní je 14. Po uplynutí tohoto času se zobrazí dialog, ve kterém je možné upravovat pravidla a následně musíte vybrat jiný režim systému HIPS.

Systém HIPS monitoruje události uvnitř operačního systému a reaguje na ně podle pravidel, která jsou strukturou podobná pravidlům Personálního firewallu. Kliknutím na **Změnit** vedle položky Pravidla otevřete Editor pravidel

systému HIPS, kde můžete pravidla prohlížet, vytvářet nová, upravovat nebo odstranit stávající.

Na následujícím příkladu si ukážeme, jak omezit nežádoucí chování aplikací:

1. Zadejte název pravidla a vyberte akci **Zablokovat** z rozbalovacího menu **Akce**,
2. Vyberte možnost **Upozornit uživatele** pro zobrazení upozornění při každém aplikování pravidla.
3. Vyberte alespoň jednu operaci, pro kterou má pravidlo platit.
4. Přejděte na záložku **Cílové aplikace**. Záložku **Zdrojové aplikace** nechte prázdnou, aby se nové pravidlo uplatnilo pro všechny aplikace, které se pokoušejí vykonat vybrané **Operace** v aplikacích uvedených v části **Nad těmito aplikacemi**,
5. Vyberte operaci **Změnit stav jiné aplikace** (všechny operace jsou popsány v nápovědě produktu, kterou vyvoláte stisknutím **klávesy F1**).
6. Pomocí tlačítka **Přidat...** přidejte jednu nebo více aplikací, které chcete ochránit,
7. Klikněte na **OK** pro uložení nového pravidla.



4.1.4.1 Rozšířená nastavení

Následující možnosti jsou užitečné pro ladění a analýzu chování aplikací:

Automaticky povolené ovladače – vybrané ovladače budou vždy načteny bez ohledu na nastavený režim filtrování, pokud nejsou blokovány uživatelským pravidlem.

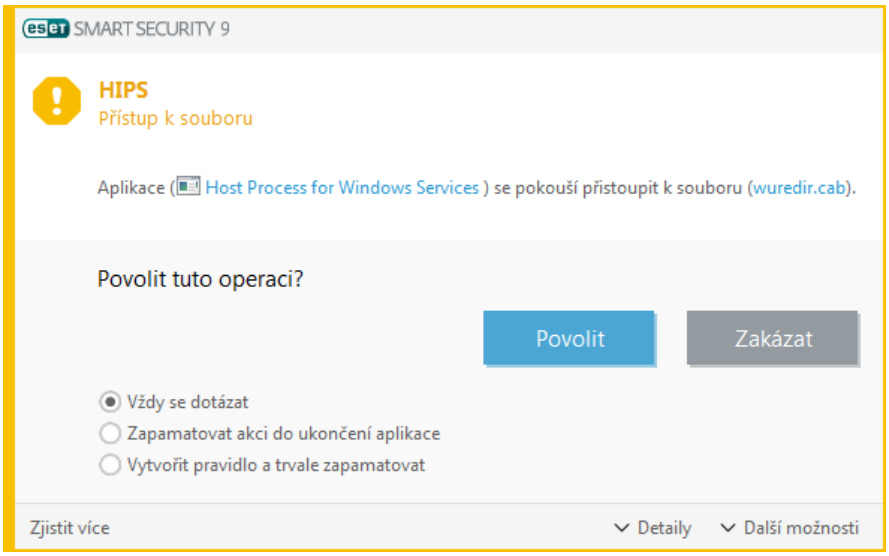
Zapisovat všechny zablokované operace do protokolu – všechny zablokované operace se zapíší do protokolu HIPS.

Upozornit na změny v seznamu aplikací automatický spouštěných při startu – při změně počtu aplikací spouštěných po startu operačního systému se zobrazí oznámení.

Nejaktuálnější verzi této nápovědy naleznete v Databázi znalostí.

4.1.4.2 Interaktivní režim HIPS

Dialogové okno s výběrem akce se zobrazí pokaždé, když je pro událost vybrána akce **Dotázat se**. Umožňuje vybrat, zda chcete operaci **Povolit** nebo **Zakázat**. Pokud nevyberete žádnou akci, použije se standardní pravidlo z již předdefinovaných.



Dialogové okno s výběrem akce umožňuje vytvoření pravidla, které má vlastnosti podle operace, která vyvolala tento dialog. Přesné parametry nového pravidla můžete nastavit po kliknutí na **Zobrazit nastavení**. Takto vytvořená pravidla se vyhodnocují stejně, jako kdyby byla zadána ručně, přesto může být pravidlo vytvořené pomocí dotazu méně specifické. To znamená, že po vytvoření pravidla může stejná operace znovu vyvolat dialogové okno, pokud se parametry z předchozího pravidla nevztahují na tuto situaci.

Aktivovaná možnost **Dočasně si zapamatovat akci pro tento proces** způsobí, že se vybraná akce (**Povolit** nebo **Zakázat**) zapamatuje pro tento proces, a použije se pokaždé, kdyby se pro operaci tohoto procesu měl zobrazit další dotazovací dialog. Tato nastavení jsou jen dočasná, platí pouze do nejbližší změny pravidel, režimu filtrování, aktualizaci modulu HIPS nebo restartu systému.

4.1.5 Herní režim

Herní režim je funkce pro uživatele, kteří nechtějí být nejen v režimu celé obrazovky rušeni vyskakujícími okny a chtějí minimalizovat veškeré nároky na zatížení procesoru. Herní režim oceníte v průběhu prezentací, kdy nechcete být rušeni aktivitami antiviru. Zapnutím této funkce zakážete zobrazování všech vyskakujících oken a všechny úlohy plánovače budou zastaveny. Samotná ochrana běží dál v pozadí, ale nevyžaduje žádné zásahy uživatele.

Herní režim můžete zapnout nebo vypnout v hlavním okně na záložce **Nastavení** > **Ochrana počítače** prostřednictvím přepínače resp. . Zapnutí herního režimu může představovat potenciální bezpečnostní riziko, a proto se ikonka ochrany na liště změní na oranžovou a zobrazí se upozornění **Herní režim je zapnutý**.

Vybráním možnosti **Automaticky zapnout Herní režim při zobrazení aplikací na celou obrazovku** se Herní režim automaticky zapne po spuštění aplikace na celou obrazovku a po jejím ukončení se vypne. Tato možnost je užitečná pro okamžité aktivování Herního režimu po spuštění hry nebo zahájení prezentace.

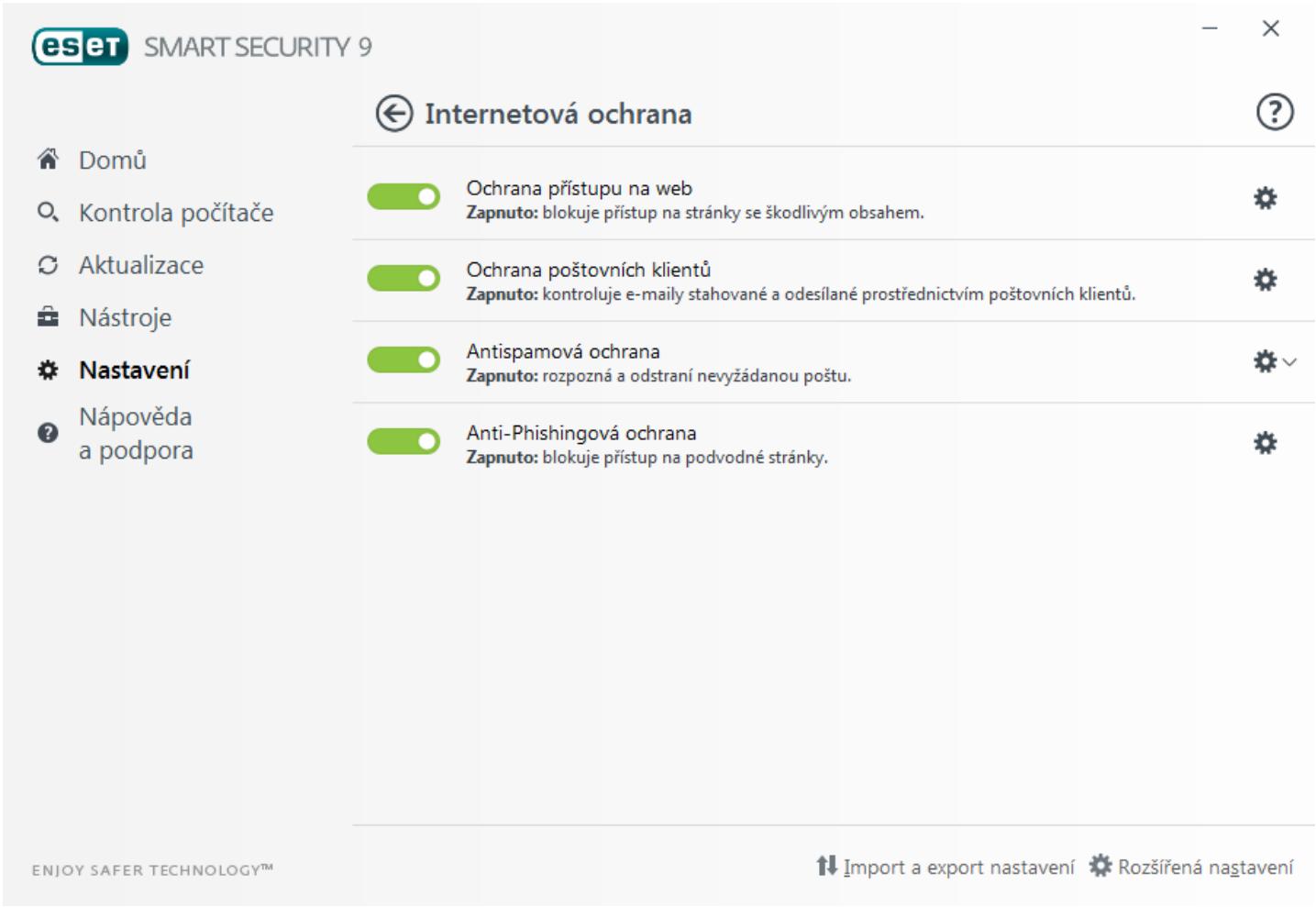
Můžete také aktivovat možnost **Automaticky vypínat Herní režim** a následně definovat interval, po jehož uplynutí se Herní režim automaticky vypne.

Poznámka: Pokud je Personální firewall v Interaktivním režimu a zapnete Herní režim, mohou se vyskytnout problémy s připojením do internetu. Toto může představovat problém například pokud spouštíte hru, která se připojuje do internetu. Je to způsobeno tím, že za normálních okolností by si firewall vyžádal potvrzení připojení (pokud nejsou definována žádná pravidla nebo výjimky pro spojení), ale v Herním režimu jsou všechna vyskakovací okna vypnuta. Řešením je definovat pravidla nebo výjimky pro každou aplikaci, která by mohla mít konflikt s tímto chováním nebo použít jiný Režim filtrování personálního firewallu. Mějte také na paměti, že pokud při zapnutém Herním režimu pracujete s aplikací nebo stránkou, která představuje potenciální riziko, pak bude tato stránka zablokována, ale nezobrazí se žádné vysvětlení nebo varování, protože jsou vypnuté všechny akce vyžadující zásah

uživatele.

4.2 Internetová ochrana

Konfiguraci webu a e-mailu naleznete na záložce **Nastavení**, po kliknutí na část **Web a mail**. Odtud se dá také dostat k podrobnějšímu nastavení programu.



Internetové připojení patří do standardní výbavy osobních počítačů a bohužel se stalo i hlavním médiem pro šíření škodlivého kódu. Proto je velmi důležité věnovat zvýšenou pozornost nastavení ochrany přístupu na web.

Klikněte na **Nastavit...** pro zobrazení nastavení webové/e-mailové/anti-phishingové/antispamové ochrany.

Ochrana poštovních klientů zabezpečuje kontrolu poštovní komunikace přijímané prostřednictvím protokolu POP3 a IMAP. Pomocí zásuvných modulů do poštovních klientů zajišťuje ESET Smart Security kontrolu veškeré komunikace těchto programů (POP3, MAPI, IMAP, HTTP).

Anti-Phishingová ochrana blokuje webové stránky, na kterých se nachází podvodný obsah. Doporučujeme ponechat anti-phishingovou ochranu zapnutou.

Antispamová ochrana zajišťuje filtrování nevyžádaných e-mailových zpráv.

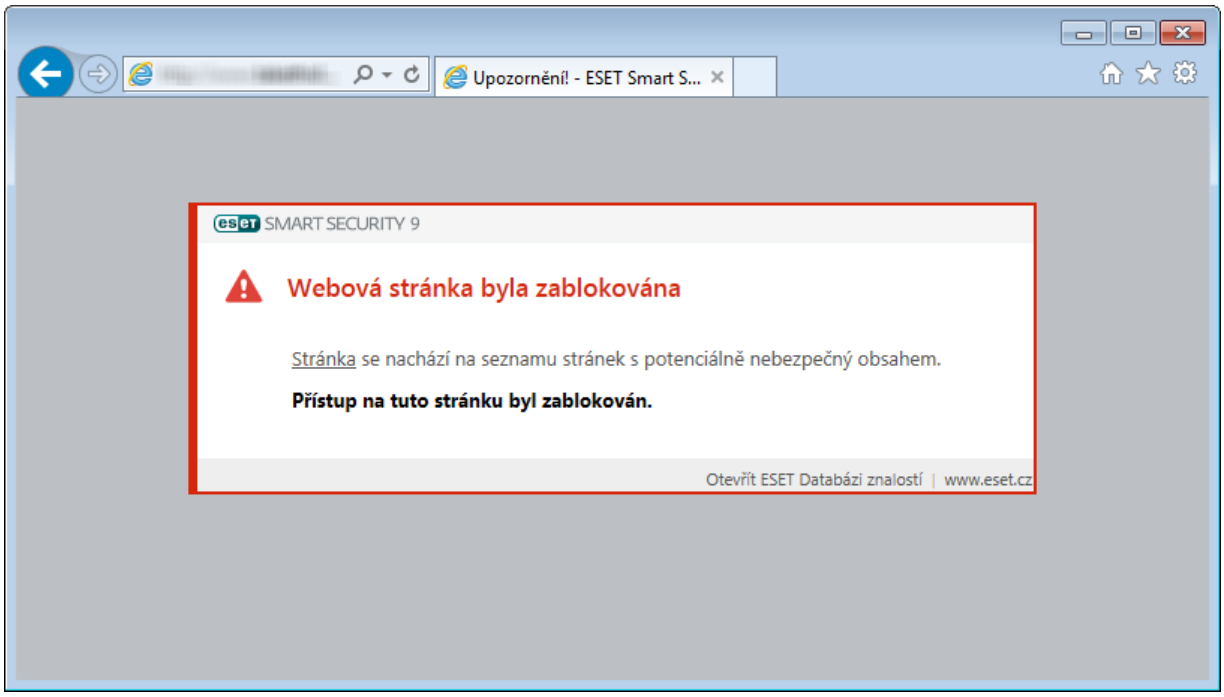
- Uživatelský seznam důvěryhodných adres – zobrazí seznam adres, které jsou považovány za důvěryhodné, např. adresy přátel, ze kterých nechodí nevyžádaná pošta.
- Uživatelský seznam spamových adres – zobrazí seznam adres, ze kterých přichází nevyžádaná pošta.
- Uživatelský seznam výjimek – zobrazí seznam adres, které mohou být falešné a zneužívané pro rozesílání nevyžádané pošty. Tyto e-mailové adresy budou vždy kontrolovány na přítomnost spamu. V seznamu výjimek se standardně nacházejí všechny adresy získané z existujícího e-mailového účtu.

Také můžete moduly webové/e-mailové/anti-phishingové/antispamové ochrany dočasně vypnout pomocí přepínače .

4.2.1 Ochrana přístupu na web

Internetové připojení se stalo u počítačů standardem. Bohužel i pro šíření škodlivého kódu. **Ochrana přístupu na web** monitoruje komunikaci mezi webovým prohlížečem a vzdáleným serverem, kdy filtruje HTTP (Hypertext Transfer Protocol) a HTTPS (šifrovanou komunikaci) na základě pravidel.

Přístup na známé webové stránky se škodlivým obsahem je zablokován ještě předtím, než je škodlivý kód stažen do počítače. Všechny ostatní webové stránky budou zkontrolovány skenovacím jádrem ThreatSense při svém načtení a zablokovány při zjištění škodlivého obsahu. K dispozici jsou dva režimy ochrany přístupu na web, blokování na základě seznamu blokovaných adres a blokování na základě obsahu.



Důrazně doporučujeme mít funkci Ochrana přístupu na web zapnutou. Podrobné možnosti konfigurace naleznete v **Rozšířeném nastavení** (dostupném po stisknutí **klávesy F5** v hlavním okně ESET Smart Security) na záložce **Web a mail** > **Ochrana přístupu na web**. Pokud je tato možnost zapnutá, známé stránky se škodlivým obsahem budou blokovány.

Dostupné jsou následující možnosti:

- **Webové protokoly** – umožňuje konfigurovat monitorování standardních protokolů používaných internetovými prohlížeči,
- **Správa URL adres** – umožňuje definovat seznamy adres webových stránek, které budou blokovány, povoleny, nebo vyloučeny z kontroly,
- **Parametry skenovacího jádra ThreatSense** – nabízí pokročilé nastavení kontroly jako jsou cíle kontroly, metody detekce ochrany přístupu na web apod.

4.2.1.1 Obecné

Zapnout ochranu přístupu na web – pokud je tato možnost vypnutá, nebude funkční ochrana přístupu na web ani Anti-Phishingová ochrana.

Poznámka: V rámci zajištění bezpečnosti nedoporučujeme tuto možnost vypínat. Tuto možnost vypněte pouze při řešení problému pokud vás k tomu vyzval specialista technické podpory.

4.2.1.2 HTTP, HTTPs

Standardně je ESET Smart Security nakonfigurován pro používání norem většiny internetových prohlížečů. Přesto je možné kontrolu HTTP konfigurovat v rozšířeném nastavení (dostupném po stisknutí **klávesy F5** v hlavním okně programu) na záložce **Web a mail** > **Ochrana přístupu na web** > **HTTP, HTTPs**. Zde můžete kontrolu aktivovat nebo deaktivovat a dále definovat čísla portů, na kterých v systému probíhá HTTP komunikace. Standardně jsou přednastaveny porty 80 (HTTP), 8080 a 3128 (pro proxy server).

ESET Smart Security podporuje také kontrolu šifrované komunikace HTTPs. Při této komunikací jsou přenášené údaje mezi serverem a klientem zašifrované. Kontrolována je komunikace šifrovaná pomocí SSL (Secure Socket Layer) nebo TLS (Transport Layer Security). Šifrovanou HTTPs komunikaci je možné filtrovat ve dvou režimech:

Nepoužívat kontrolu protokolu HTTPs – šifrovaná komunikace nebude kontrolována,

Používat kontrolu protokolu HTTPs pro vybrané porty – kontrolována bude pouze komunikace na portech definovaných v sekci Weboví a poštovní klienti a používají porty definované v sekci **Porty používané protokolem HTTPs**. Standardně se kontroluje komunikace na portu 443.

Šifrovaná komunikace se standardně nekontroluje. Pro aktivování kontroly šifrované komunikace přejděte do sekce Kontrola protokolu SSL/TLS v Rozšířeném nastavení (dostupném po stisknutí **klávesy F5** v hlavním okně programu). Následně na záložce **Web a mail** > **Filtrování protokolů** > **SSL** zaškrtněte možnost **Zapnout kontrolu protokolu SSL/TLS**.

4.2.1.3 Správa URL adres

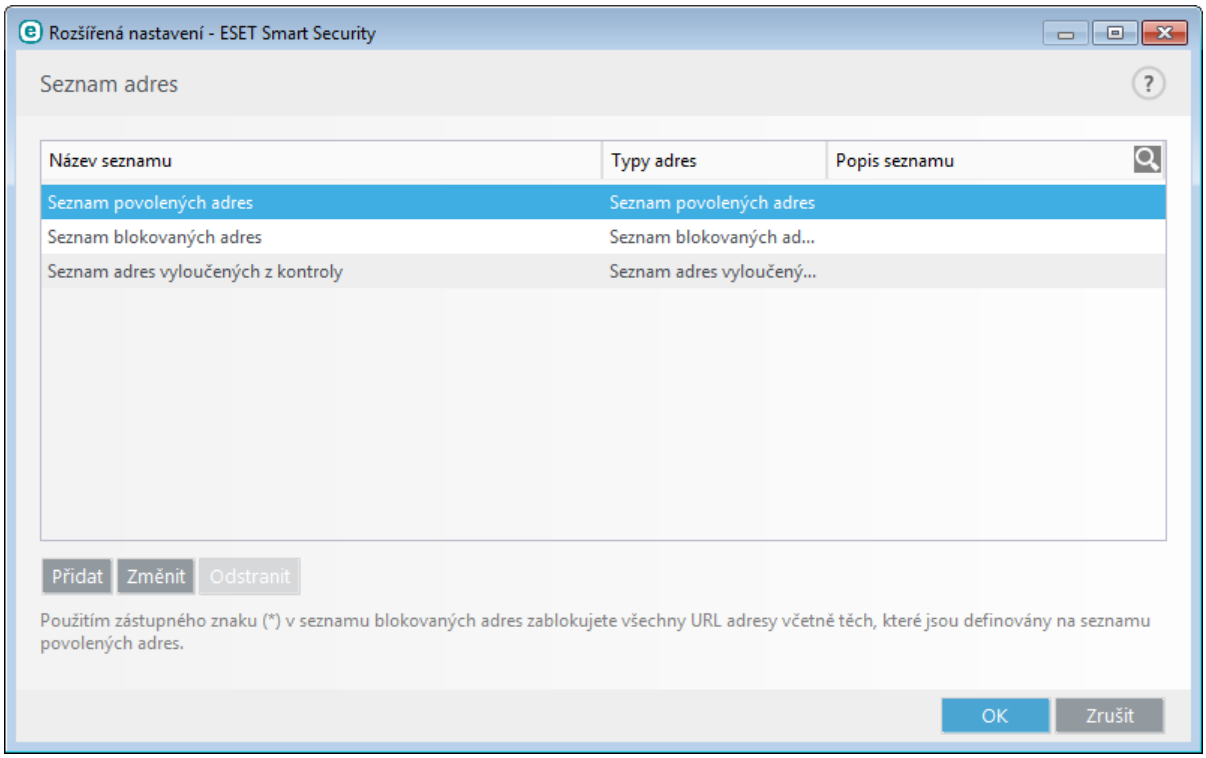
Správa URL adres umožňuje definovat seznamy adres webových stránek, které budou blokovány, povoleny, nebo vyloučeny z kontroly.

Webové stránky zařazené na **Seznamu blokovaných adres** nebudou dostupné, na rozdíl od adres na **Seznamu povolených adres**. Webové stránky zařazené na **Seznamu adres vyloučených z kontroly** nebudou kontrolovány na přítomnost škodlivého kódu.

Možnost Povolit filtrování protokolu SSL/TLS musí být aktivní, pokud chcete filtrovat HTTPS adresy. V opačném případě by byl zakázán pouze přístup na nešifrovanou verzi webové stránky.

V seznamech můžete používat speciální znaky * (hvězdička) a ? (otazník). Přičemž znak * nahrazuje libovolný řetězec a znak ? nahrazuje libovolný znak. Vyloučené adresy se nekontrolují proti hrozbám a proto by měl seznam výjimek obsahovat pouze ověřené a důvěryhodné adresy. Je potřeba dbát opatrnosti při používání speciálních znaků v tomto seznamu. Pro více informací, jak bezpečně přidat celou doménu včetně jejich subdomén přejděte do kapitoly Přidání masky adresy/domény. Pro aktivování seznamu vyberte možnost **Seznam je aktivní**. Při aplikování adresy ze seznamu je možné nastavit zobrazení upozornění zaškrtnutím možnosti **Upozornit při aplikování adresy ze seznamu**.

Pokud chcete zablokovat všechny HTTP adresy kromě těch definovaných na **Seznamu povolených adres**, použijte při tvorbě seznamu zástupný znak *.



Ovládací prvky

Přidat – umožňuje vytvořit nový seznam. To je užitečné, pokud chcete adresy rozdělit do logických skupin. Například jeden seznam blokovaných adres může obsahovat adresy z veřejných blacklistů, a druhý vámi definované adresy. V takovém případě je správa seznamu externích adres mnohem snadnější.

Změnit – upraví existující seznam adres.

Odstranit – odebere existující seznam. Toto platí pouze na ručně vytvořené seznamy, nikoli předdefinované.

4.2.2 Ochrana poštovních klientů

4.2.2.1 Poštovní klienti

Integrace ESET Smart Security do poštovních klientů zvyšuje úroveň ochrany před škodlivým kódem obdrženým prostřednictvím e-mailových zpráv. Pokud používáte poštovního klienta, který ESET Smart Security podporuje, je vhodné integraci povolit. Při integraci dochází k vložení panelu nástrojů programu ESET Smart Security do poštovního klienta (panel nástrojů není dostupný pro nejnovější verze Windows Live Mail), což přispívá k efektivnější kontrole e-mailových zpráv. Konkrétní možnosti integrace naleznete v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu) na záložce **Web a mail** > **Ochrana poštovních klientů** > **Poštovní klienti**.

Integrace s poštovními klienty

Modul ochrany poštovních klientů podporuje Microsoft Outlook, Outlook Express, Windows Mail a Windows Live Mail. Ochrana je zajišťována pomocí zásuvného doplňku v těchto programech. Hlavní výhodou je nezávislost na použitém protokolu. Pokud jsou zprávy šifrovány, virový skener je dostává ke kontrole již dešifrované. Úplný seznam dostupných poštovních klientů a jejich verzí naleznete v ESET Databázi znalostí.

Pokud není nastavena integrace, e-mailová komunikace je stále chráněna modulem ochrany poštovních klientů (POP3, IMAP).

Možnost **Vypnout kontrolu při změně obsahu složek s doručenou poštou** doporučujeme použít v případě, že pociťujete zpomalení při práci s poštovním klientem. Uvedená situace může nastat například, že přijímáte zprávy z úložiště zpráv prostřednictvím Kerio Outlook Connector.

Kontrolovat tyto zprávy

Příchozí zprávy – zapnutí/vypnutí kontroly přijatých zpráv.
Odchozí zprávy – zapnutí/vypnutí kontroly odesílaných zpráv.
Čtené zprávy – zapnutí/vypnutí kontroly prohlížených zpráv.

S infikovanými zprávami provést následující akci

Žádná akce – program upozorní na zprávy s infikovanými přílohami, avšak neprovede žádnou akci.
Vymazat zprávu – program upozorní na infikované přílohy a odstraní celou zprávu.
Přesunout zprávu do složky s odstraněnými zprávami – program bude přesouvat infikované zprávy do složky s vymazanými zprávami.
Přesunout zprávu do složky – program bude přesouvat infikované zprávy do vybrané složky.

Složka – definujte vlastní složku, do které přesouvat infikované zprávy.

Opakovat kontrolu po aktualizaci – zapnutí/vypnutí opakované kontroly zpráv po aktualizaci virové databáze.
Zohlednit výsledky kontroly jiných modulů – zapnutí/vypnutí zohlednění výsledku kontroly jiným modulem.

4.2.2.2 Poštovní protokoly

Protokol POP3 a IMAP je nejrozšířenější protokol určený pro příjem e-mailové komunikace prostřednictvím poštovního klienta. ESET Smart Security zajišťuje ochranu těchto protokolů zcela nezávisle na používaném klientovi.

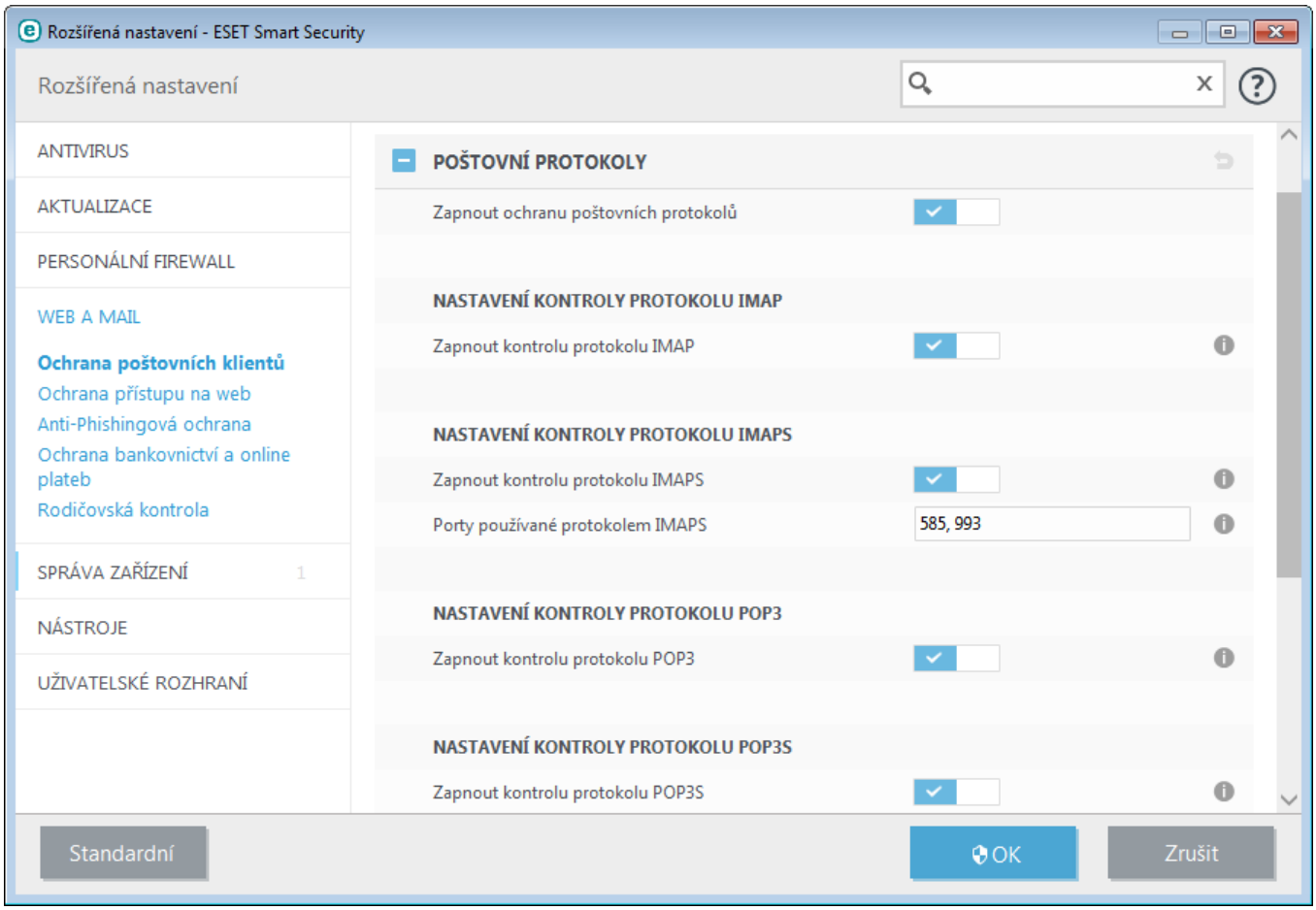
Konfiguraci kontroly protokolu IMAP/IMAPS a POP3/POP3S naleznete v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu) na záložce **Web a mail** > **Ochrana poštovních klientů** > **Poštovní protokoly**. Pro zapnutí tohoto modulu použijte přepínač **Zapnout ochranu poštovních protokolů**.

Ve Windows Vista a novějších je komunikace na protokolech IMAP a POP3 automaticky zjišťována a kontrolována na všech portech. Ve Windows XP jsou kontrolovány pouze definované **Porty používané protokolem IMAP/POP3** a aplikace označené jako Weboví a poštovní klienti.

ESET Smart Security podporuje kontrolu protokolů IMAPS a POP3S, které používají šifrovaný kanál pro výměnu informací mezi klientem a serverem. ESET Smart Security kontroluje komunikaci využívající protokol SSL (Secure Socket Layer) a TLS (Transport Layer Security). Komunikace bude kontrolována pouze na definovaných **Portech používaných protokolem IMAPS/POP3S**, v závislosti na verzi systému.

Šifrovaná komunikace se standardně nekontroluje. Pro aktivování kontroly šifrované komunikace přejděte v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu) na záložku **Filtrování protokolů** > Kontrola protokolu SSL/TLS a aktivujte možnost **Povolit filtrování protokolu SSL/TLS**.

Šifrovaná komunikace se standardně nekontroluje. Pro aktivování kontroly šifrované komunikace přejděte do sekce Kontrola protokolu SSL/TLS v Rozšířeném nastavení (dostupném po stisknutí **klávesy F5** v hlavním okně programu). Následně na záložce **Web a mail** > **Filtrování protokolů** > **SSL** zaškrtněte možnost **Zapnout kontrolu protokolu SSL/TLS**.



4.2.2.3 Upozornění a události

Ochrana poštovních klientů zabezpečuje kontrolu poštovní komunikace přijímané prostřednictvím protokolu POP3 a IMAP. Pomocí zásuvného doplňku do Microsoft Outlook a dalších e-mailových klientů je zajištěna kontrola veškeré komunikace (POP3, MAPI, IMAP, HTTP). Při kontrole přijímaných zpráv jsou použity veškeré pokročilé metody kontroly obsažené ve skenovacím jádře ThreatSense. Tím je zajištěna detekce nebezpečných programů ještě před aktualizací virových databází. Kontrola protokolu POP3 a IMAP je nezávislá na typu poštovního klienta.

Možnosti konfigurace pro tuto funkci jsou dostupné v **Rozšířeném nastavení** (po stisknutí klávesy F5 v hlavním okně) na záložce **Web a mail** > **Ochrana poštovních klientů** > **Upozornění a události**.

Parametry skenovacího jádra ThreatSense – rozšířené nastavení kontroly umožňuje vybrat cíle kontroly, metody detekce atd.

Do kontrolovaných zpráv je možné přidávat podpis s informacemi o výsledku kontroly. Textové upozornění můžete **Přidávat do přijatých a čtených zpráv** nebo pouze **Přidávat do odchozích zpráv**. Samozřejmě, na tyto podpisy se nelze zcela spoléhat, protože nemusí být doplněny do problematických HTML zpráv a také mohou být zfalšovány viry. Přidávání podpisu můžete nastavit zvlášť pro přijaté a čtené zprávy a zvlášť pro odesílané zprávy. Možná nastavení jsou následující:

- **Nepřidávat do zpráv** – program nebude přidávat podpisy do žádných kontrolovaných zpráv,
- **Přidávat pouze do infikovaných zpráv** – program bude přidávat podpisy pouze do infikovaných zpráv,
- **Přidávat do všech kontrolovat zpráv** – program bude přidávat podpisy do všech kontrolovaných zpráv.

Přidávat do předmětu odchozích infikovaných zpráv – vypnutím této funkce se nebude do předmětu infikované zprávy přidávat informace o tom, že obsahuje infiltraci. Tato funkce se dá využít pro snadné filtrování infikovaných zpráv podle předmětu, pokud to poštovní klient umožňuje. Zároveň zvyšuje důvěryhodnost zprávy a v případě výskytu infiltrace nabízí cenné informace o úrovni hrozby pro příjemce i odesílatele.

Šablona přidávaná do předmětu infikovaných zpráv – upravte tuto šablonu, pokud chcete změnit formát předpony předmětu infikovaného e-mailu. Tato funkce přidá k původnímu předmětu zprávy "Ahoj" předponu "*[virus]*" a výsledný předmět bude: "*[virus] Ahoj*". Proměnná *%VIRUSNAME%* představuje detekovanou hrozbou.

4.2.2.4 Integrace s poštovními klienty

Integrace ESET Smart Security s poštovními klienty zvyšuje úroveň aktivní ochrany před škodlivým kódem obsaženým v e-mailových zprávách. V případě, že je daný poštovní klient podporován, je vhodné povolit jeho integraci s ESET Smart Security. Při integraci dochází k vložení panelu nástrojů programu ESET Smart Security do poštovního klienta, což přispívá k efektivnější kontrole e-mailových zpráv. Konkrétní možnosti integrace jsou dostupné v **Rozšířeném nastavení** (po stisknutí klávesy F5 v hlavním okně programu) ve větvi **Web a mail** > **Ochrana poštovních klientů** > **Integrace s poštovními klienty**.

V tomto dialogu je možné aktivovat integraci s podporovanými poštovními klienty, kterými v současné verzi jsou Microsoft Outlook, Outlook Express, Windows Mail a Windows Live Mail. Pro kompletní výpis podporovaných klientů a jejich verzí si přečtěte článek v ESET Databázi znalostí.

Možnost **Vypnout kontrolu při změně obsahu složek s doručenou poštou** doporučujeme použít v případě, že pociťujete zpomalení při práci s poštovním klientem. Uvedená situace může nastat například, že přijímáte zprávy z úložiště zpráv prostřednictvím Kerio Outlook Connector.

Pokud není vybrána integrace, e-mailová komunikace bude chráněna modulem ochrany poštovních klientů (POP3, IMAP).

4.2.2.4.1 Nastavení ochrany poštovních klientů

Modul ochrany poštovních klientů podporuje Microsoft Outlook, Outlook Express, Windows Mail a Windows Live Mail. Ochrana je zajišťována pomocí zásuvného doplňku v těchto programech. Hlavní výhodou je nezávislost na použitém protokolu. Pokud jsou zprávy šifrovány, virový skener je dostává ke kontrole již dešifrované.

4.2.2.5 Kontrola protokolu POP3, POP3s

Protokol POP3 je nejrozšířenější protokol určený pro příjem e-mailové komunikace prostřednictvím poštovního klienta. ESET Smart Security zajišťuje ochranu tohoto protokolu nezávisle na používaném klientovi.

Modul zajišťující kontrolu se zavádí při startu operačního systému a po celou dobu je zaveden v paměti. Pro správné fungování ověřte, zda je modul zapnutý. Kontrola protokolu POP3 je prováděna automaticky bez nutnosti konfigurace poštovního klienta. Standardně je kontrolována komunikace na portu 110, v případě potřeby je možné přidat i jiný používaný port. Čísla portů se oddělují čárkou.

Šifrovaná komunikace se standardně nekontroluje. Pro aktivování kontroly šifrované komunikace přejděte do sekce Kontrola protokolu SSL/TLS v Rozšířeném nastavení (dostupném po stisknutí **klávesy F5** v hlavním okně programu). Následně na záložce **Web a mail** > **Filtrování protokolů** > **SSL** zaškrtněte možnost **Zapnout kontrolu protokolu SSL/TLS**.

V této sekci můžete nastavit kontrolu protokolů POP3 a POP3s.

Aktivovat kontrolu protokolu POP3 – zapne sledování poštovní komunikace přes POP3 na přítomnost škodlivého softwaru.

Porty používané protokolem POP3 – nastavení kontrolovaných portů poštovní komunikace přes POP3 (standardně 110).

ESET Smart Security také podporuje kontrolu protokolu POP3s. Při této komunikaci jsou přenášeny údaje mezi serverem a klientem přes šifrovaný kanál. ESET Smart Security kontroluje komunikaci šifrovanou metodami SSL (Secure Socket Layer) a TLS (Transport Layer Security).

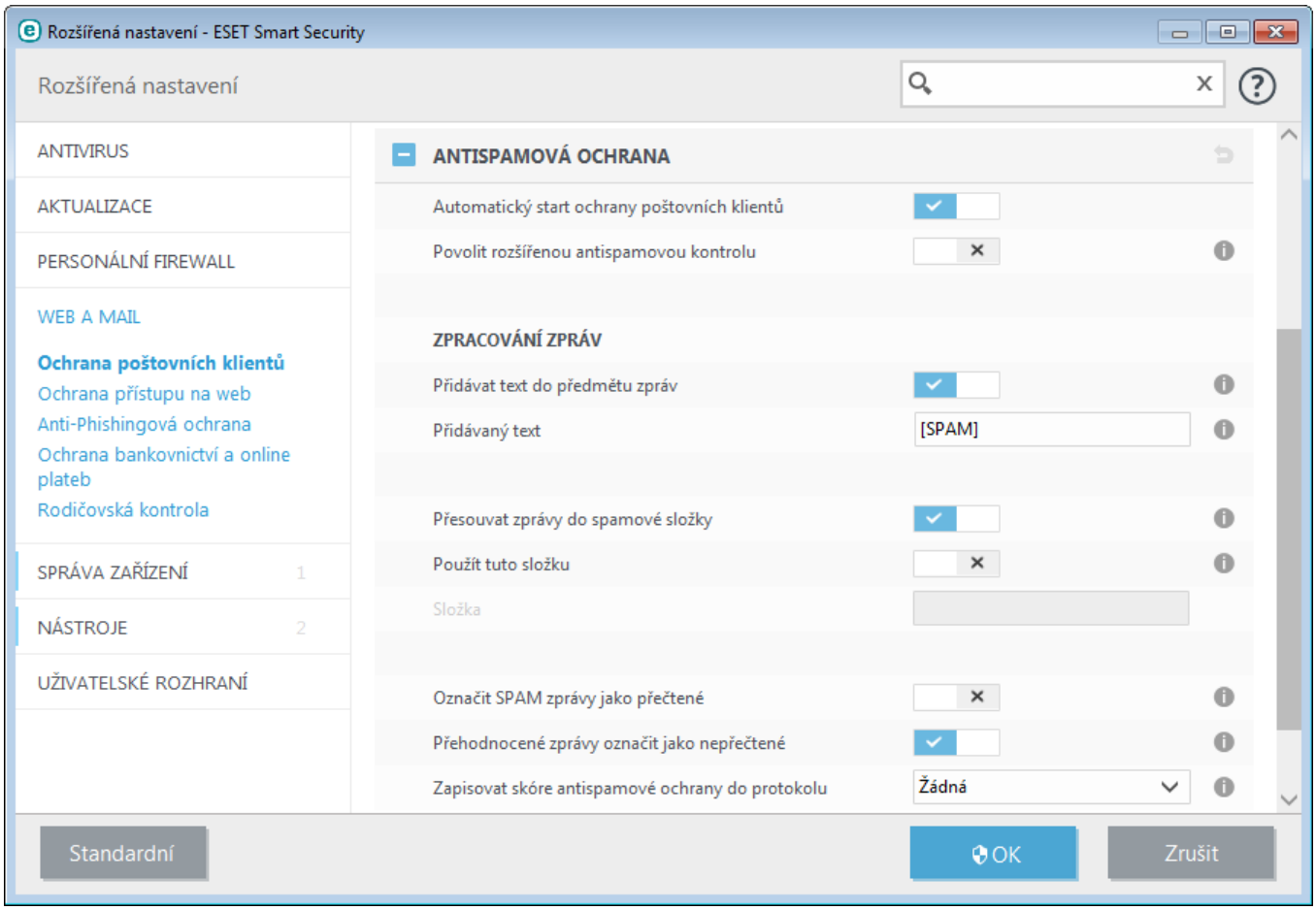
Nepoužívat kontrolu protokolu POP3s – šifrovaná komunikace nebude kontrolována.

Používat kontrolu protokolu POP3s pro vybrané porty – kontrolovaná bude pouze komunikace přes porty definované v nastavení **Porty používané protokolem POP3s.**

Porty používané protokolem POP3S – nastavení kontrolovaných portů poštovní komunikace přes POP3s (standardně 995).

4.2.2.6 Antispamová ochrana

V současnosti mezi největší problémy e-mailové komunikace patří nevyžádaná pošta – spam, který tvoří až 80 % e-mailové komunikace. Antispamová ochrana slouží k ochraně právě před tímto problémem. Obsahuje kombinaci několika účinných principů, které zajišťují filtrování příchozí pošty.



Základní metodou rozpoznávání nevyžádané pošty je využívání seznamu důvěryhodných (whitelist) a spamových adres (blacklist). Mezi důvěryhodné adresy jsou automaticky zařazeny všechny z adresáře e-mailového klienta a seznam adres se dále rozšiřuje o adresy, které označíte jako důvěryhodné.

Hlavním principem je rozpoznávání spamu na základě vlastností e-mailových zpráv. Přijatá zpráva je prověřena na základě pravidel (vzorky zpráv, statistická heuristika, rozpoznávací algoritmy a další jedinečné metody) a podle výsledku se rozhodně, zda se jedná o spam nebo ne.

Automatický start ochrany poštovních klientů – pomocí této možnosti zapnete/vypnete automatický start antispamové ochrany poštovních programů.

Povolit rozšířenou antispamovou kontrolu – pravidelně se budou stahovat další antispamová data pro zajištění přesnějších výsledků filtrování.

Antispamová ochrana produktu ESET Smart Security umožňuje nastavit různé parametry pro práci se seznamy adres. Možnosti jsou následující:

Zpracování zpráv

Přidávat text do předmětu zprávy – umožňuje přidávat vlastní text do předmětu e-mailové zprávy klasifikované jako spam. Standardně "[SPAM]".

Přesouvat zprávy do spamové složky – zapne/vypne přesouvání zpráv do složky s nevyžádanou poštou.

Použít tuto složku – vyberte tuto možnost, pokud chcete spam přesouvat do jiné, než předefinované složky.

Označit SPAM zprávy jako přečtené – nevyžádanou zprávu označí jako přečtenou, což vám umožní koncentrovat pozornost na legitimní doručené zprávy.

Přehodnocené zprávy označit jako nepřečtené – zprávy, které byly dříve označeny jako spam, budou po novém vyhodnocení jako legitimní označeny jako nepřečtené.

Zapisovat skóre antispamové ochrany do protokolu – antispamové jádro ESET Smart Security přiřazuje každé zkontrolované zprávě skóre. Zpráva je zároveň zaznamenána do protokolu antispamu, který je dostupný v hlavním okně **ESET Smart Security** na záložce **Nástroje** > **Protokoly** > **Antispamová ochrana**.

- **Nezapisovat** – sloupec Skóre bude v protokolu antispamové ochrany prázdný.
- **Zapisovat pouze pro přehodnocené zprávy a zprávy označené jako SPAM** – vyberte tuto možnost, pokud chcete zapisovat spam skóre pouze pro zprávy označené jako SPAM.
- **Zapisovat pro všechny zprávy** – všechny zprávy budou mít zaznamenáno spam skóre.

Poznámka: Po kliknutí pravým tlačítkem na zprávu umístěnou ve složce spam můžete z kontextového menu vybrat možnost **Přehodnotit vybrané zprávy jako NENÍ spam**. Poté bude zpráva přesunuta do složky s doručenou poštou. Podobným způsobem můžete přesunout zprávu v doručené poště mezi SPAM vybráním možnosti **Přehodnotit vybrané zprávy jako SPAM**.

Poznámka: ESET Smart Security podporuje antispamovou ochranu pro aplikace Microsoft Outlook, Outlook Express, Windows Mail a Windows Live Mail.

4.2.3 Filtrování protokolů

Antivirová ochrana aplikačních protokolů je prováděna prostřednictvím skenovacího jádra ThreatSense, které obsahuje všechny pokročilé metody detekce škodlivého softwaru. Kontrola pracuje zcela nezávisle na použitém internetovém prohlížeči, nebo poštovním klientovi. Pro kontrolu šifrované komunikace (SSL) přejděte do sekce **Web a mail** > **Kontrola protokolu SSL/TLS**.

Zapnout kontrolu obsahu aplikačních protokolů – pokud tuto možnost vypnete některé moduly ESET Smart Security, které závisí na této funkci (například Ochrana přístupu na web, Ochrana poštovních klientů, Anti-Phishing, Filtrování obsahu webu), nebudou fungovat.

Vyloučené aplikace – umožňuje vyloučit konkrétní aplikaci z filtrování protokolů. To může být užitečné při řešení problémů.

Vyloučené IP adresy – umožňuje vyloučit konkrétní adresu z filtrování protokolů. To může být užitečné při řešení problémů

Internetové prohlížeče a poštovní klienti – Tato možnost je dostupná pouze na operačním systému XP/2003 a umožňuje vybrat aplikace jejichž komunikace bude filtrována, bez ohledu na používaný port.

4.2.3.1 Weboví a poštovní klienti

Poznámka: Na systémech Windows Vista s nainstalovaným Service Packem 1, Windows 7 a Windows Server 2008 je použit odlišný způsob kontroly komunikace (je využita nová architektura Windows Filtering Platform), než na starších systémech. Z tohoto důvodu není nastavení **Weboví a poštovní klienti** na těchto systémech dostupné.

Bezpečnost při prohlížení webových stránek je vzhledem k velkému množství škodlivého kódu důležitou součástí ochrany počítače. Zranitelnosti prohlížečů a podvodné odkazy dokáží zavést škodlivý kód do systému bez vědomí uživatele. Z tohoto důvodu je v ESET Smart Security věnována pozornost bezpečnosti internetových prohlížečů. Každá aplikace, která přistupuje k síti, může být označena jako internetový prohlížeč. Zaškrtávací pole má dva stavy:

- **Prázdné** – komunikace této aplikace se sítí je filtrována pouze podle portů.
- **Označeno fajfkou** – komunikace této aplikace se sítí je filtrována vždy (i v případě, že je nastaven jiný port).

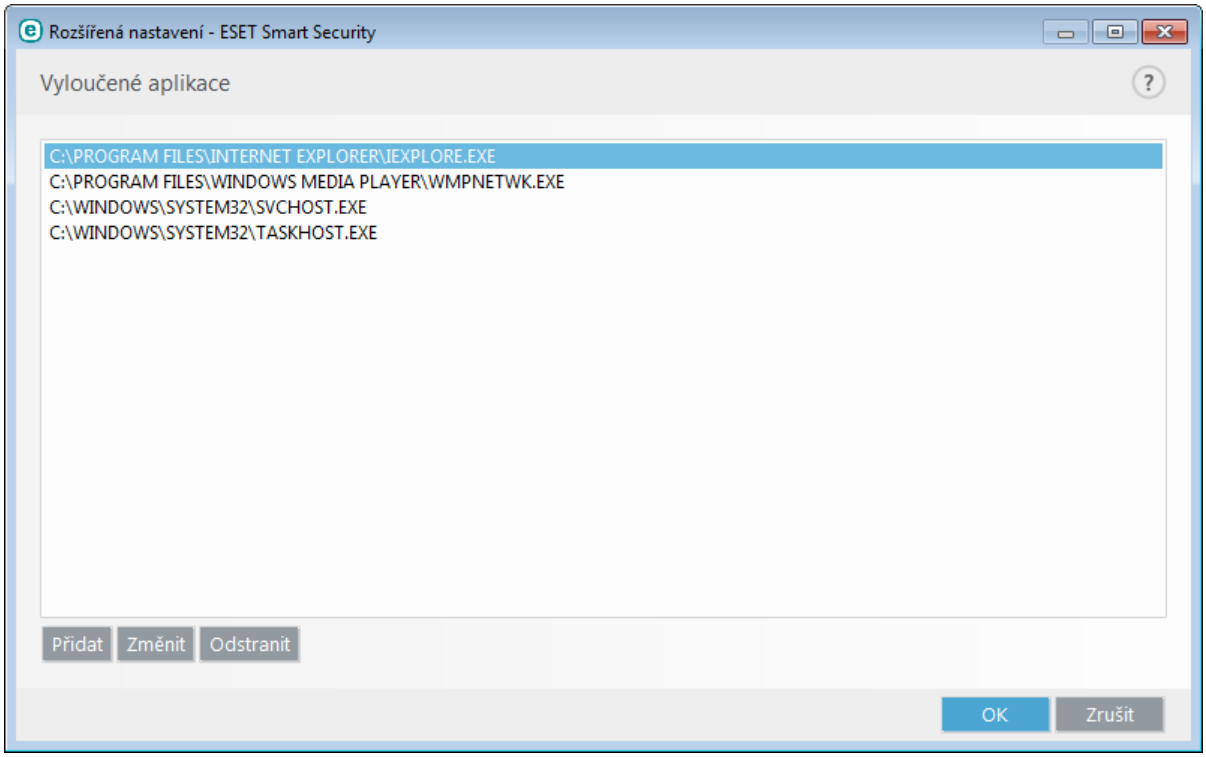
4.2.3.2 Vyloučené aplikace

V tomto dialogovém okně vyberte aplikace, které chcete vyloučit z kontroly filtrování protokolů. HTTP, POP3 a IMAP komunikace vybraných aplikací nebude kontrolována na přítomnost hrozeb. Tuto možnost doporučujeme použít pouze ve výjimečných případech, například pokud aplikace v důsledku kontroly komunikace nepracuje správně.

Spuštěné aplikace a běžící služby se zobrazí automaticky. Pomocí tlačítka **Přidat** ručně vyberte cestu k aplikaci, kterou chcete přidat do seznamu výjimek filtrování protokolů.

Změnit – upraví existující aplikaci.

Odstranit – odebere vybranou aplikaci ze seznamu.



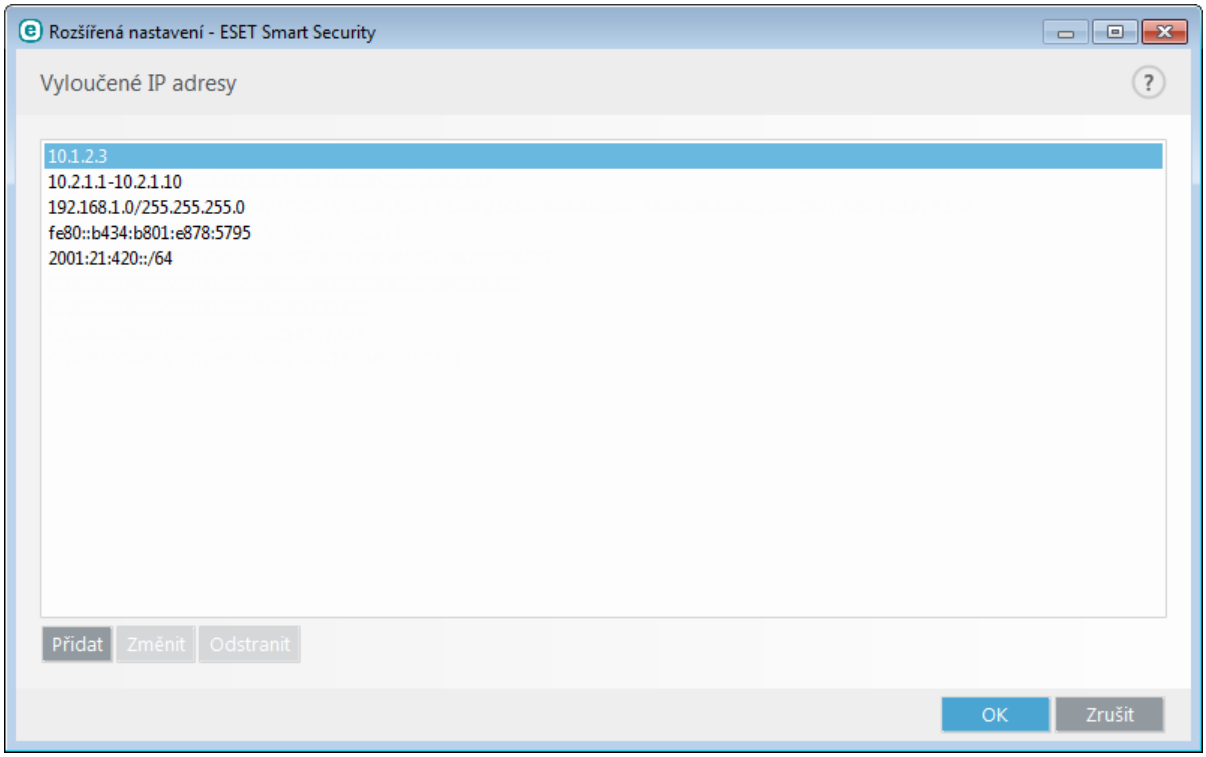
4.2.3.3 Vyloučené IP adresy

IP adresy uvedené v tomto seznamu budou vyloučeny z filtrování protokolů. Oboustranná komunikace protokolů HTTP, POP3 a IMAP z těchto IP adres nebude kontrolována na hrozby. Doporučujeme používat tuto možnost pouze v případě důvěryhodných IP adres.

Přidat – klikněte pro přidání IP adresy/rozsahu adres/podsítě vzdálené strany, kterou chcete vyloučit z filtrování.

Změnit – upraví existující IP adresu v seznamu.

Odstranit – odebere vybrané IP adresy ze seznamu.



4.2.3.3.1 Přidání adresy IPv4

Umožní přidání IP adresy/rozsahu adres/podsítě vzdáleného zařízení, pro které budou daná pravidla aplikována. Internetový protokol (IP) verze 4 je starší než IPv6, ale v současnosti je stále nejrozšířenější.

Samostatná adresa – slouží pro zadání samostatné adresy počítače, pro který má pravidlo platit (například *192.168.0.10*).

Rozsah adres – vytvoří pravidla pro více počítačů po zadání rozsahu IP adres těchto počítačů, pro které má pravidlo platit (například *192.168.0.1* až *192.168.0.99*).

Podsíť – umožní zadat podsíť skupiny počítačů pomocí IP adresy a masky.

Příklad: *255.255.255.0* je maska podsítě pro prefix *192.168.1.0/24*, což znamená rozsah adres od *192.168.1.1* do *192.168.1.254*.

4.2.3.3.2 Přidání IPv6 adresy

Umožní přidání IPv6 adresy/podsítě vzdáleného zařízení, pro které budou daná pravidla aplikována. Tato nejnovější verze Internetového Protokolu (IP) nahrazuje starší verzi 4.

Samostatná adresa – slouží pro zadání samostatné adresy počítače, pro který má pravidlo platit (například *2001:718:1c01:16:214:22ff:fec9:ca5*).

Podsíť – umožní zadat podsíť skupiny počítačů pomocí IP adresy a masky (například *2002:c0a8:6301:1::1/64*).

4.2.3.4 Kontrola protokolu SSL/TLS

ESET Smart Security umožňuje také kontrolu protokolů zapouzdřených v protokolu SSL. Kontrolu můžete přizpůsobit podle toho, zda je certifikát využíván danou SSL komunikací důvěryhodný, neznámý, nebo je zařazen na seznamu certifikátů, pro které se nebude vykonávat kontrola obsahu v protokolu SSL.

Povolit kontrolu protokolu SSL/TLS – pokud je tato možnost aktivní, bude se provádět kontrola každé šifrované komunikace pomocí protokolu SSL.

K dispozici jsou následující **režimy filtrování protokolu SSL/TLS**:

Automatický režim – vyberte tuto možnost, pokud chcete kontrolovat veškerou komunikaci chráněnou protokolem SSL kromě komunikace chráněné certifikáty vyloučených z kontroly. Při navázání komunikace využívající zatím neznámý certifikát, který je důvěryhodně podepsán, nebudete upozorněni a komunikace bude automaticky filtrována. Při přístupu k serveru využívající nedůvěryhodný certifikát označený jako důvěryhodný, komunikace bude povolena a přenášený obsah bude filtrován.

Interaktivní režim – při přístupu k nové stránce chráněné protokolem SSL (s neznámým certifikátem) se zobrazí dialogové okno s výběr akce. Pomocí tohoto režimu můžete vytvořit seznam SSL certifikátů, které chcete vyloučit z kontroly.

Aplikace jejichž SSL komunikace je kontrolována – pomocí této možnosti můžete vytvořit seznam aplikací, u kterých bude komunikace SSL kontrolována.

Seznam známých certifikátů – pomocí této možnosti můžete přidat do programu důvěryhodné certifikáty.

Nekontrolovat komunikaci s důvěryhodnými doménami – pokud je tato možnost aktivní, komunikace mezi servery používajícími EV (Extended Validation) certifikáty nebude kontrolována. V takovém případě je jisté, že nejde o phishingovou stránku.

Blokovat šifrovanou komunikaci používající zastaralý protokol SSL v2 – komunikace využívající starší verzi protokolu SSL bude automaticky blokována.

Kořenový certifikát

Kořenový certifikát – pro správné fungování kontroly SSL komunikace ve webových prohlížečích a poštovních klientech je potřeba přidat kořenový certifikát společnosti ESET do seznamu známých kořenových certifikátů (vydavatelů). Možnost **Přidat kořenový certifikát do známých prohlížečů** by měla být zapnuta. Pomocí této možnosti zajistíte automatické přidání kořenového certifikátu společnosti ESET do známých prohlížečů (například prohlížeče Opera nebo Firefox). Do prohlížečů využívající systémové úložiště kořenových certifikátů se certifikát přidá automaticky (například prohlížeče Internet Explorer).

V případě nepodporovaných prohlížečů certifikát exportujte pomocí tlačítka **Zobrazit certifikát** > **Detaily** > **Kopírovat do souboru** a následně jej ručně importujte do prohlížeče.

Platnost certifikátu

Pokud nelze ověřit platnost certifikátu pomocí systémového úložiště (TRCA) – v některých případech nelze certifikát webové stránky ověřit pomocí systémového úložiště kořenových certifikátů (TRCA). To znamená, že certifikát je někým samostatně podepsán (například administrátorem webového serveru nebo malou firmou) a považování tohoto certifikátu za důvěryhodný nemusí vždy představovat riziko. Většina velkých obchodních společností (například banky) používají certifikát podepsaný certifikační autoritou (Trusted Root Certification Authorities). Pokud vyberete možnost **Dotázat se uživatele na platnost certifikátu** (tato možnost je nastavena standardně), při navázání šifrované komunikace se zobrazí okno s výběrem akce. Pomocí možnosti **Zakázat komunikaci využívající daný certifikát** se vždy zablokuje komunikace s webovou stránkou využívající nedůvěryhodný certifikát.

Pokud je certifikát neplatný nebo poškozený – znamená to, že certifikátu vypršela platnost nebo nebyl správně podepsán. V tomto případě doporučujeme **zakázat komunikaci využívající daný certifikát**.

Pomocí **seznamu známých certifikátů** můžete přizpůsobit chování ESET Smart Security, při detekci konkrétních SSL certifikátů.

4.2.3.4.1 Certifikáty

Pro správné fungování kontroly SSL komunikace ve webových prohlížečích a poštovních klientech je potřeba přidat kořenový certifikát společnosti ESET do seznamu známých kořenových certifikátů (vydavatelů). Možnost Přidat kořenový certifikát do známých prohlížečů by měla být zapnuta. Pomocí této možnosti zajistíte automatické přidání kořenového certifikátu společnosti ESET do známých prohlížečů (například prohlížeče Opera nebo Firefox). Do prohlížečů využívající systémové úložiště kořenových certifikátů se certifikát přidá automaticky (například prohlížeče Internet Explorer).

V případě nepodporovaných prohlížečů certifikát exportujte pomocí tlačítka **Zobrazit certifikát** > **Detaily** > **Kopírovat do souboru** a následně jej ručně importujte do prohlížeče.

V některých případech nelze certifikát webové stránky ověřit pomocí systémového úložiště kořenových certifikátů (TRCA). To znamená, že certifikát je někým samostatně podepsán (například administrátorem webového serveru nebo malou firmou) a považování tohoto certifikátu za důvěryhodný nemusí vždy představovat riziko. Většina velkých obchodních společností (například banky) používají certifikát podepsaný certifikační autoritou (Trusted Root Certification Authorities). Pokud vyberete možnost **Dotázat se uživatele na platnost certifikátu** (tato možnost je nastavena standardně), při navázání šifrované komunikace se zobrazí okno s výběrem akce. Pokud se certifikát nenachází v TRCA, zobrazí se červené okno, v opačném případě bude zelené.

Pomocí možnosti **Zakázat komunikaci využívající daný certifikát** vždy zablokujete komunikaci s webovou stránkou využívající nedůvěryhodný certifikát.

Pokud je certifikát neplatný nebo poškozený, znamená to, že certifikátu vypršela platnost nebo nebyl správně podepsán. V tomto případě doporučujeme **zakázat komunikaci využívající daný certifikát**.

4.2.3.4.2 Seznam známých certifikátů

Pomocí **seznamu známých certifikátů** můžete přizpůsobit chování ESET Smart Security, při detekci konkrétních SSL certifikátů. V tomto seznamu naleznete certifikáty, pro které jste v Interaktivním režimu nastavili zapamatování vybrané akce. Seznam naleznete v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu) na záložce **Web a mail** > **Kontrola protokolu SSL/TLS** > **Seznam známých certifikátů**.

Dialogové okno se **seznamem známých certifikátů** obsahuje:

Sloupce

Název – název certifikátu.

Vydavatel certifikátu – jméno autora certifikátu.

Předmět certifikátu – identifikace entity asociované s veřejným klíčem uloženým v poli předmět veřejného klíče.

Přístup – pro povolení nebo zablokování komunikace využívající daný certifikát bez ohledu na to, zda je důvěryhodný, vyberte možnost **Povolit** nebo **Blokovat**. V případě možnosti **Automaticky** budou důvěryhodné certifikáty povoleny, a v nedůvěryhodných bude muset uživatel vybrat akci. Pokud nastavíte **Dotázat se**, vždy se uživateli zobrazí výzva s výběrem akce.

Kontrolovat – pro kontrolu nebo ignorování komunikace využívající daný certifikát vyberte možnost **Kontrolovat** nebo **Ignorovat**. V případě možnosti **Automaticky** se bude komunikace kontrolovat v automatickém režimu filtrování a výzva s výběrem akce se uživateli zobrazí v interaktivním režimu. Pokud nastavíte **Dotázat se**, vždy se uživateli zobrazí výzva s výběrem akce.

Ovládací prvky

Přidat – certifikát můžete přidat ručně ve formátu *.cer*, *.crt* nebo *.pem* a to buď přímo ze souboru nebo externího zdroje po zadání URL.

Změnit – klikněte pro úpravu již existujícího certifikátu.

Odstranit – klikněte pro odebrání vybraného certifikátu.

OK/Zrušit – pro uložení změn klikněte na tlačítko **OK**, v opačném případě klikněte na tlačítko **Zrušit**.

4.2.3.4.3 Aplikace jejichž SSL komunikace je kontrolována

Pomocí **seznamu aplikací, u kterých je kontrolována SSL komunikace** můžete přizpůsobit chování ESET Smart Security, při detekci konkrétních SSL certifikátů. V tomto seznamu naleznete certifikáty, pro které jste v Interaktivním režimu nastavili zapamatování vybrané akce. Seznam naleznete v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu) na záložce **Web a mail** > **Kontrola protokolu SSL/TLS** > **Seznam známých certifikátů**.

Dialogové okno se seznamem aplikací, u kterých je kontrolována SSL komunikace obsahuje:

Sloupce

Aplikace – název aplikace.

Kontrolovat – pro kontrolu nebo ignorování komunikace využívající daný certifikát vyberte možnost **Kontrolovat** nebo **Ignorovat**. V případě možnosti **Automaticky** se bude komunikace kontrolovat v automatickém režimu filtrování a výzva s výběrem akce se uživateli zobrazí v interaktivním režimu. Pokud nastavíte **Dotázat se**, vždy se uživateli zobrazí výzva s výběrem akce.

Ovládací prvky

Přidat – certifikát můžete přidat ručně ve formátu *.cer*, *.crt* nebo *.pem* a to buď přímo ze souboru nebo externího zdroje po zadání URL.

Změnit – klikněte pro úpravu již existujícího certifikátu.

Odstranit – klikněte pro odebrání vybraného certifikátu.

OK/Zrušit – pro uložení změn klikněte na tlačítko **OK**, v opačném případě klikněte na tlačítko **Zrušit**.

4.2.4 Anti-Phishingová ochrana

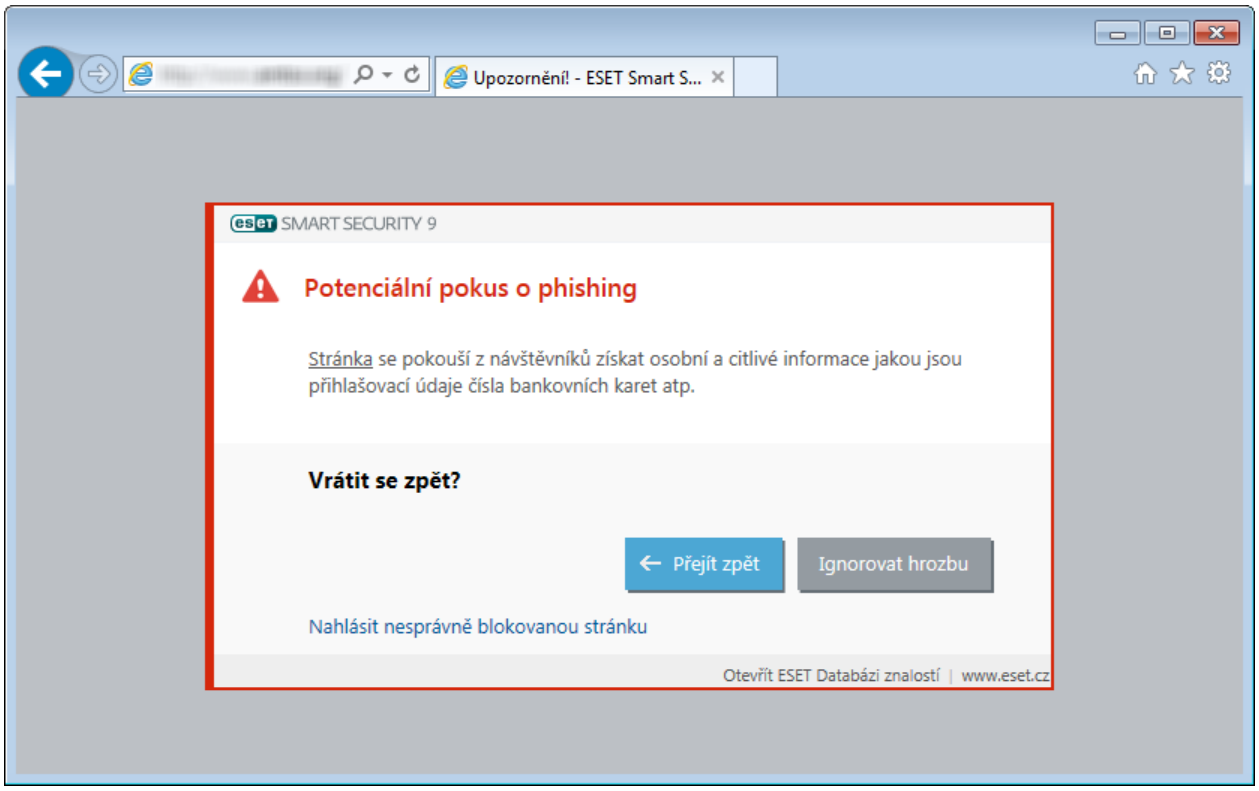
Termín phishing definuje kriminální činnost, která využívá sociální inženýrství (manipulace uživatelů za účelem získání citlivých dat). Nejčastěji je vyžadován přístup k bankovnímu účtu nebo PIN. Více informací naleznete ve slovníku pojmů). ESET Smart Security obsahuje anti-phishingovou ochranu, která blokuje internetové stránky s tímto obsahem.

Důrazně doporučujeme aktivovat Anti-Phishingovou ochranu programu ESET Smart Security. To provedete v **Rozšířeném nastavení** (dostupném po stisknutím klávesy F5 v hlavním okně programu) na záložce **Web a mail** > **Anti-Phishing**.

Podrobnější informace o fungování Anti-Phishingové ochrany naleznete v ESET Databázi znalostí.

Přístup na stránky s phishingovým obsahem

Pokud otevřete stránku se škodlivým obsahem, zobrazí se v internetovém prohlížeči níže uvedené upozornění. Pokud přesto chcete stránku otevřít, klikněte na tlačítko **Pokračovat na stránku** (nedoporučujeme).



Poznámka: Potenciální phishingové stránky, které jsou zařazeny na seznam povolených výjimek, budou standardně znovu nepřístupné za několik hodin. Pokud chcete stránky povolit natrvalo, použijte Správce URL adres – v **Rozšířeném nastavení** (dostupném po stisknutím klávesy F5 v hlavním okně programu) přejděte na záložku **Web a mail** > **Ochrana přístupu na web** > **Správa URL adres** a upravte **Seznam povolených adres**.

Nahlášení phishingové stránky

Pokud narazíte na stránku se škodlivým obsahem, zašlete prosím daný odkaz k analýze do virové laboratoře ESET prostřednictvím této stránky.

Poznámka: Předtím než odešlete stránku do společnosti ESET se ujistěte, že splňuje alespoň jedno z níže uvedených kritérií:

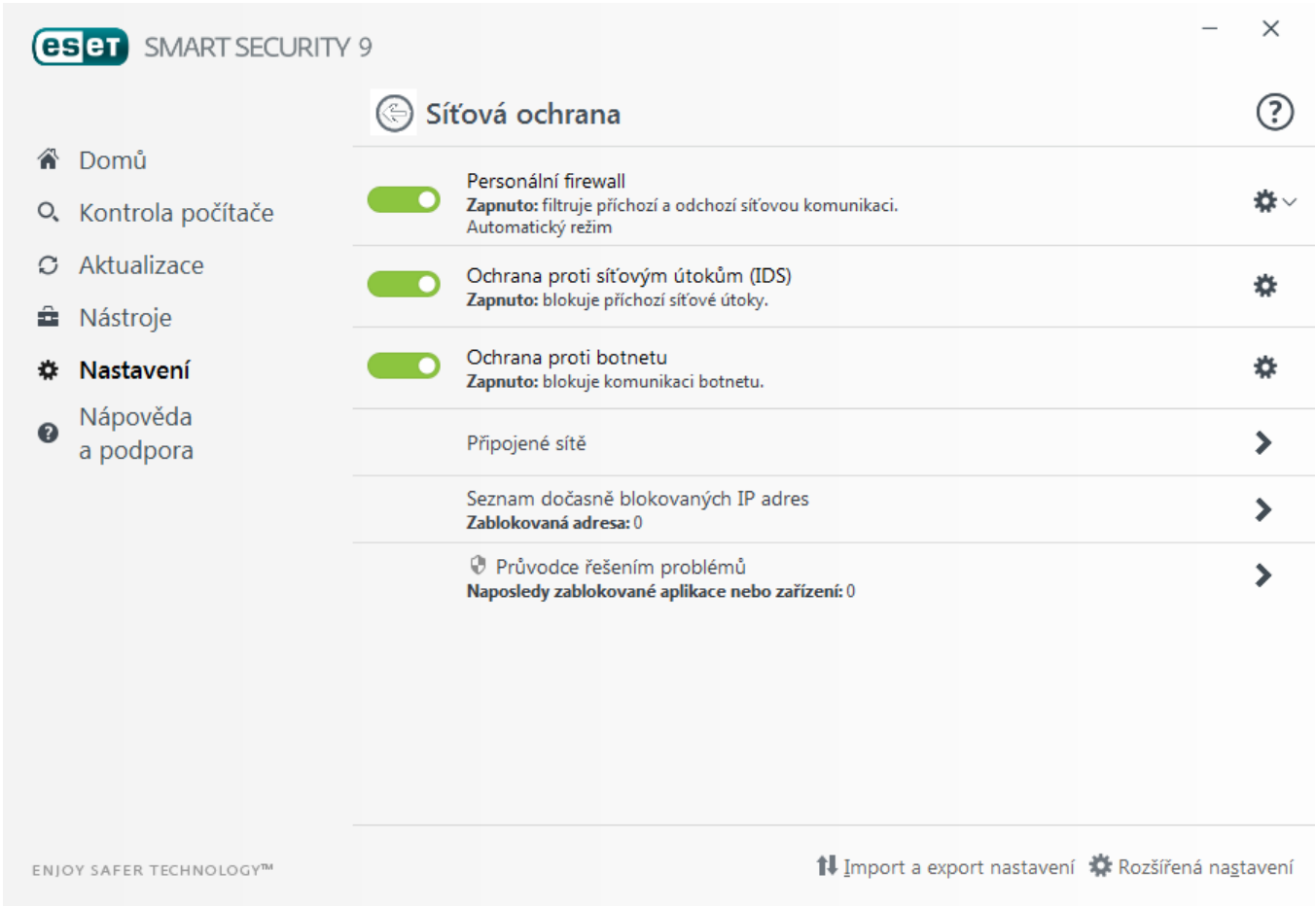
- stránka není detekována jako škodlivá,
- stránka je chybně detekována jako škodlivá. V tomto případě použijte tento odkaz.

Případně můžete odkaz na webovou stránku odeslat e-mailem na adresu samples@eset.com. Nezapomeňte vyplnit předmět e-mailu a přiložte maximální možné množství informací o dané stránce (jak jste se k ní dostali, od koho jste odkaz na ní obdrželi apod.)

4.3 Síťová ochrana

Personální firewall zajišťuje kontrolu všech spojení mezi sítí a daným systémem, přičemž umožňuje na základě definovaných pravidel tato jednotlivá spojení povolit nebo zablokovat. Chrání před útoky ze vzdálených počítačů a umožňuje blokování některých potenciálně nebezpečných služeb. Dále zajišťuje funkci IDS/IPS a kontrolu obsahu přenášeného aplikačními protokoly, díky čemuž dokáže zabránit zobrazení potenciálně nechtěného obsahu.

Nastavení personálního firewallu naleznete na záložce **Nastavení** v části **Síť**, kde je možné rychle měnit režim filtrování. Detailní nastavení zpřístupníte kliknutím na ozubené kolečko > **Nastavit...**, případně jej v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu) naleznete na záložce **Personální firewall**.



Po kliknutí na ozubené kolečko vedle **Personálního firewallu** se zobrazí kontextové menu s následujícími možnostmi:

Nastavit... – otevře rozšířené nastavení Personálního firewallu, kde můžete detailně definovat režimy filtrování.

Blokovat veškerou komunikaci – Každá příchozí a odchozí komunikace je Personálním firewallem bez upozornění uživatele zablokována. Použití této možnosti je vhodné při podezření na možná kritická bezpečnostní rizika, která vyžadují odpojení systému od sítě. Pokud je komunikace zablokována, obnovíte ji po kliknutí na **Povolit veškerou komunikaci**.

Dočasně vypnout firewall – je opačnou funkcí k výše zmiňovanému blokování veškeré komunikace. Při použití této možnosti je filtrování komunikace Personálním firewallem úplně vypnuto a všechna příchozí i odchozí spojení jsou povoleny. Pokud je firewall vypnutý, obnovíte jej po kliknutí na **Zapnout firewall**.

Automatický režim – (pokud je aktivován jiný režim filtrování) – kliknutím provedete změnu režimu filtrování na automatický.

Interaktivní režim – (pokud je aktivován jiný režim filtrování) – kliknutím provedete změnu režimu filtrování na interaktivní.

Ochrana proti síťovým útokům (IDS) – tato funkce analyzuje obsah síťové komunikace a chrání vás před síťovými

útoky. Ochranu proti síťovým útokům můžete dočasně deaktivovat pomocí přepínače  .

Ochrana proti botnetu – tato funkce zajišťuje ochranu před škodlivým kódem, který se počítač snaží zapojit do botnetu. Ochranu proti zapojení do botnetu můžete dočasně deaktivovat pomocí přepínače  .

Připojené sítě – v této části se zobrazí sítě, ke kterým jste připojeni. Po kliknutí na ozubené kolečko můžete nastavit režim ochrany v síti.

Seznam dočasně blokovaných IP adres – zobrazí seznam IP adres, ze kterých byl zjištěn útok na tento počítač, a z tohoto důvodu byla dočasně zablokována komunikace z těchto adres. Pro více informací klikněte na tuto možnost a následně stiskněte klávesu F1.

Průvodce řešením problémů – pomáhá s řešením problémů se síťovou komunikací, kterou ovlivnil ESET Personální firewall. Pro více informací přejděte do kapitoly Průvodce řešením problémů.

4.3.1 Personální firewall

Personální firewall sleduje veškerou příchozí i odchozí síťovou komunikaci z počítače. Na základě pravidel povoluje nebo blokuje konkrétní komunikaci. Úkolem firewallu je zablokovat příchozí útoky ze vzdálených počítačů a blokovat nežádoucí služby a aplikace. Dále zajišťuje antivirovou ochranu HTTP, POP3 a IMAP protokolů. Jedná se tak o velmi důležitou součást při zabezpečení počítače.

Zapnout ochranu proti síťovým útokům (IDS) – tato funkce analyzuje obsah síťové komunikace a chrání vás před síťovými útoky. Detailní možnosti ochrany jsou dostupné v sekci IDS a rozšířená nastavení.

Zapnout ochranu proti zapojení do botnetu – tato funkce analyzuje síťovou komunikaci a protokoly, které využívá škodlivý kód při komunikaci s botnetem.

Personální firewall v ESET Smart Security může pracovat v několika režimech filtrování. Režimy filtrování naleznete v **Rozšířeném nastavení** (dostupném po stisknutí **klávesy F5** v hlavním okně programu) na záložce **Personální firewall**. Chování personálního firewallu záleží na vybraném režimu. Vybraný režim také ovlivňuje míru interakce uživatele.

Filtrování personálního firewallu je možné nastavit do jednoho z následujících režimů.

Automatický režim – je přednastaven po instalaci. Je určen pro uživatele, kteří preferují rychlé a pohodlné fungování Personálního firewallu bez nutnosti definování pravidel. Vlastní pravidla vytvářet můžete, ale nejsou pro běh Automatického režimu vyžadována. Tento režim povoluje veškerou komunikaci z daného systému směrem ven a blokuje nevyžádanou komunikaci směrem dovnitř (kromě komunikace v důvěryhodné zóně, stejně tak povolených služeb v IDS a rozšířeném nastavení a příchozí komunikace odpovídající na nedávnou odchozí komunikaci na stejnou vzdálenou stranu).

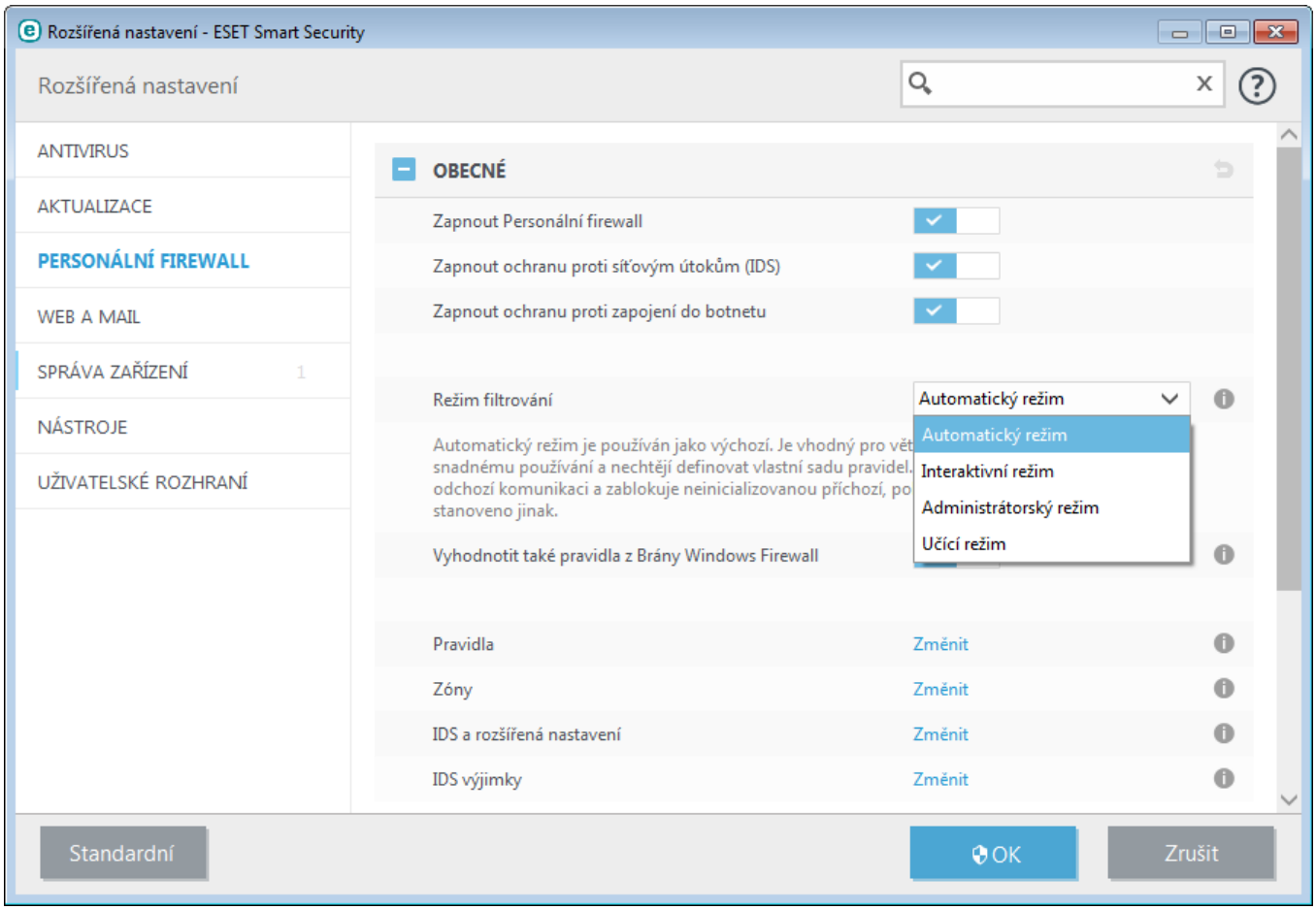
Interaktivní režim – představuje komfortní možnost nastavení Personálního firewallu na míru podle požadavků uživatele. V případě zjištění jakékoli komunikace, na kterou není možné aplikovat žádné existující pravidlo, se uživateli zobrazí dialogové okno s výběrem akce. Následně je možné tuto komunikaci povolit nebo zamítnout, přičemž z tohoto rozhodnutí můžete vytvořit nové pravidlo. V takovém případě bude každá další komunikace tohoto typu v budoucnu povolena nebo zablokována, podle tohoto pravidla.

Administrátorský režim – blokuje každé spojení, pro které neexistuje povolující pravidlo. Zkušený uživatel tak může povolit pouze požadované bezpečné spojení a Personální firewall bude blokovat veškerou ostatní neznámou komunikaci.

Učící režim – automaticky vytváří pravidla a je vhodný pro prvotní konfiguraci Personálního firewallu. Vytvoření pravidel proběhne bez interakce uživatele, protože ESET Smart Security pravidla vytvoří na základě předem definovaných parametrů. Tento režim není bezpečný a doporučujeme jej používat pouze krátkodobě po instalaci, dokud se nevytvoří pravidla pro veškerou nutnou komunikaci.

Pomocí Profilů můžete ovlivnit chování ESET Smart Security Personálního firewallu.

Vyhodnotit také pravidla z Brány Windows Firewall – po aktivování této možnosti se při vyhodnocování síťové komunikace budou uplatňovat také pravidla definovaná v Bráně Windows Firewall. V automatickém režimu firewallu bude komunikace zakázaná pravidly ESET Personálního firewallu povolena, pokud je povolena v Bráně Windows Firewall.



Pravidla – zobrazí dialogové okno, pomocí kterého můžete upravovat, na základě kterých Personální firewall povoluje/blokuje komunikaci.

Zóny – pomocí této možnosti můžete definovat zóny tvořené IP adresami.

IDS a rozšířené nastavení – slouží pro konfiguraci rozšířeného filtrování a funkcí IDS, které detekuje mnoho typů útoků a zranitelností.

IDS výjimky – umožňuje vytvořit IDS výjimky a upravit odezvu programu na výskyt síťových útoků.

4.3.1.1 Učící režim

Personální firewall ESET Smart Security obsahuje učící režim, ve kterém je pro každou komunikaci vytvořeno a uloženo odpovídající pravidlo. Vytváření pravidel probíhá bez interakce s uživatelem, protože jsou vytvářeny na základě definovaných parametrů.

Tento režim není bezpečný a doporučujeme jej používat pouze pro prvotní konfiguraci Personálního firewallu.

Po aktivování Učícího režim získáte v **Rozšířeném nastavení** (dostupném po stisknutí klávesy **F5** v hlavním okně programu)> na záložce **Personální firewall** > **Nastavení Učícího režimu** přístup k následujícím možnostem konfigurace:

Varování: V učícím režimu Personální firewall nefiltruje komunikaci. Povolená je veškerá odchozí a příchozí komunikace. Počítač v tomto režimu není plnohodnotně chráněn Personálním firewallem.

Typ komunikace – pro každý typ komunikace můžete vybrat speciální zásady pro vytváření pravidel. Existují čtyři typy komunikace:

Příchozí komunikace z důvěryhodné zóny – vzdálený počítač z důvěryhodné zóny se pokouší komunikovat s lokální aplikaci běžící na počítači.

Odchozí komunikace do důvěryhodné zóny – lokální aplikace se pokouší komunikovat s jiným počítačem v lokální síti nebo s jinou sítí v důvěryhodné zóně.

Příchozí komunikace z internetu – vzdálený počítač se pokouší komunikovat s aplikací běžící na počítači.

Odchozí komunikace do internetu – aplikace běžící na počítači se pokouší komunikovat se vzdáleným počítačem.

V každé sekci můžete definovat parametry nově vytvářených pravidel:

Přidat lokální port – číslo lokálního portu síťového spojení. Protože se většinou pro odchozí spojení generují náhodná čísla portů, je vhodné při vytváření pravidla pro příchozí spojení definovat pouze lokální port.

Přidat aplikaci – název lokální aplikace. Je doporučeno použít tehdy, pokud chcete do pravidla zahrnout kompletní komunikaci specifikované aplikace. Tedy např. povolit komunikaci pro prohlížeč webových stránek, poštovního klienta apod.

Přidat vzdálený port – číslo vzdáleného portu síťového spojení. Příkladem může být povolení nebo zakázání konkrétní služby se známým číslem portu, např. HTTP – 80, POP3 – 110 apod.

Přidat vzdálenou IP adresu / důvěryhodnou zónu – vzdálená IP adresa nebo celá zóna adres může být použita jako parametr při vytváření nového pravidla, které se použije na všechny síťové spojení mezi lokálním systémem a těmito adresami. Vhodné použít v případě, pokud chcete definovat akce pro konkrétní počítač nebo skupinu počítačů v síti.

Maximální počet různých pravidel pro jednu aplikaci – pokud aplikace komunikuje více směry (z různých portů, na různé IP adresy a pod.), poté pro ně firewall v učícím režimu vytvoří odpovídající počet pravidel. Tímto je možné omezit počet pravidel, které mohou být vytvořeny pro jednu aplikaci.

4.3.2 Profily firewallu

Profily jsou účinným nástrojem pro ovlivnění chování Personálního firewallu ESET Smart Security. Pro každé pravidlo můžete definovat, v jakém profilu je platné. Pokud není pro pravidlo vybrán žádný profil, platí pravidlo pro každý profil. Můžete si vytvořit několik profilů s odlišnými pravidly, mezi kterými se lze jednoduše přepínat.

Kliknutím na tlačítko **Změnit** vedle položky **Seznam profilů** zobrazíte dialogové okno **Profily firewallu**, ve kterém můžete definovat jednotlivé profily.

Síťový adaptér můžete nastavit tak, že pro každou připojenou síť se použije jiný profil. Rovněž můžete přiřadit konkrétní profil dané síti v sekci **Rozšířeném nastavení** (F5) > **Personální firewall** > **Známé sítě**. Vyberte síť ze seznamu **Známých sítí**, klikněte na tlačítko **Upravit** a z rozbalovacího menu **Profil firewallu** vyberte profil, který chcete síti přiřadit. Pokud síť nebude mít přiřazen žádný profil, použije se výchozí profil. Pokud síťový adaptér nemá nastaven žádný síťový profil, použije se výchozí profil v podle připojené sítě. Pokud neexistuje žádný síťový profil nebo profil k síťovému adaptéru, použije se globální výchozí profil. Pro přiřazení profilu síťovému adaptéru, klikněte na tlačítko **Změnit** vedle položky **Profily přiřazené síťovým adaptérům**. Následně vyberte síťový adaptér, klikněte na tlačítko **Změnit** a vyberte profil z rozbalovacího menu **Výchozí profil firewallu**.

Při automatickém přepnutí na nový profil se v pravém dolním rohu obrazovky zobrazí informační bublina.

4.3.2.1 Profily přiřazené síťovým adaptérům

Přepínáním profilů můžete rychle měnit chování firewallu. Vlastní pravidla mohou být platná pouze pro některé profily. Všechny síťové adaptéry v počítači se automaticky zobrazí v dialogovém okně **Síťové adaptéry**.

Sloupce

Název – název síťového adaptéru.

Výchozí profil firewallu – pokud se připojíte k síti, která nemá definovaný profil, nebo síťový adaptér nemá nastaven profil, použije se výchozí profil.

Preferovaný síťový profil – pokud je aktivní možnost **Preferovaný profil firewallu připojené sítě**, na síťový adaptér se použije profil firewallu přiřazený připojené síti.

Ovládací prvky

Přidat – klikněte pro přidání nového síťového adaptéru.

Změnit – klikněte pro úpravu již existujícího síťového adaptéru.

Odstranit – vyberte síťový adaptér, který chcete odstranit a klikněte na toto tlačítko.

OK/Zrušit – klikněte na tlačítko **OK** pro uložení změn, v opačném případě klikněte na tlačítko **Zrušit**.

4.3.3 Jak nastavit a používat pravidla

Pravidla představují seznam podmínek, podle kterých jsou testována všechna síťová spojení, a jsou k nim přiřazené akce. Můžete tedy definovat, jaká akce se má provést se spojením, které splňuje podmínky daného pravidla. Nastavení pravidel filtrování se nachází v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu) na záložce **Personální firewall** > **Obecné**. Některá předdefinovaná pravidla naleznete v sekci **povolené služby** (IDS a rozšířené nastavení), kde je můžete deaktivovat.

Na rozdíl od předchozí verze ESET Smart Security jsou pravidla nově vyhodnocována ze shora dolů. Pro každou komunikaci se provede první vyhovující pravidlo. To je důležitá změna oproti předchozí verzi, kdy priorita pravidel byla určována automaticky a konkrétní pravidla měla vyšší prioritu než pravidla obecná.

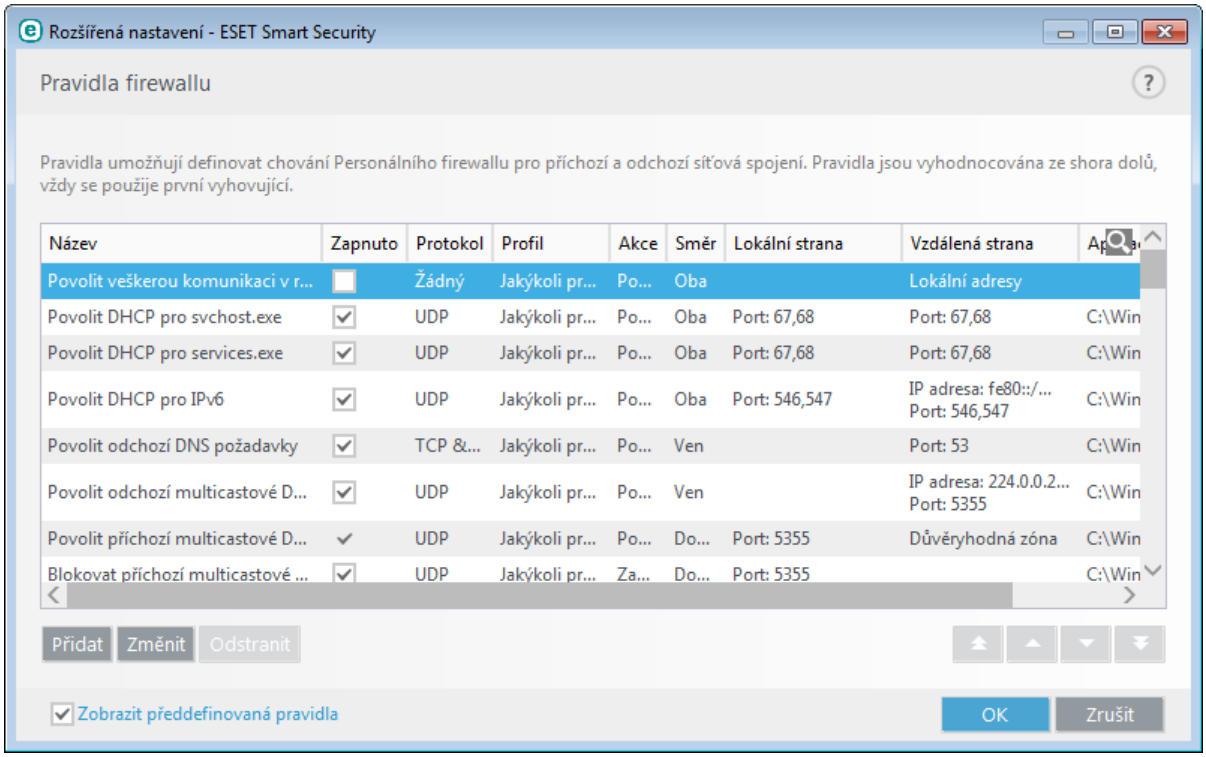
Z hlediska směru komunikace je možné provést rozdělení spojení na příchozí a odchozí. Příchozí spojení je iniciováno na vzdálené straně a snaží se navázat spojení s lokální stranou. V případě odchozího spojení je situace opačná, tedy lokální strana navazuje spojení se vzdáleným počítačem.

V případě zjištění neznámé komunikace je potřeba zvážit, zda ji povolit nebo zamítnout. Nevyžádané, nezabezpečené nebo zcela neznámé spojení představuje pro systém bezpečnostní riziko. Při takové komunikaci je vhodné věnovat pozornost především vzdálené straně a aplikaci, která se pokouší navázat toto spojení. Mnoho infiltrací odesílá soukromá data nebo stahuje další škodlivé aplikace na počítač. Právě tato skrytá spojení je možné pomocí Personálního firewallu odhalit a zakázat.

4.3.3.1 Nastavení pravidel

Dialogové okno **Pravidla firewallu** zobrazíte kliknutím na **Změnit** vedle položky **Pravidla** v sekci **Obecné**. Spravovat jednotlivá pravidla můžete pomocí tlačítek **Přidat**, **Změnit**, **Odstranit** v dolní části okna. Pro pořadí vyhodnocování pravidel použijte tlačítka **Nahoru/Výše/Dolů/Níže**.

Tip: Pro rychlé nalezení konkrétního pravidla můžete použít **Vyhledávání**. Vyhledávat je možné podle názvu pravidla, protokolu nebo portu.



Sloupce

Zapnuto – informace o tom, zda je dané pravidlo aktivní nebo nikoli.

Název – název pravidla.

Protokol – informace, pro který internetový protokol pravidlo platí.

Profil – profil, pro který pravidlo platí.

Akce – akci, která se s komunikací provede (zablokovat/povolit/dotázat se).

Směr – směr komunikace (příchozí/odchozí/oba).

Lokální – IP adresa a port lokálního počítače.

Vzdálená – IP adresa a port vzdáleného počítače.

Aplikace – název aplikace, pro kterou platí pravidlo.

Ovládací prvky

Přidat – vytvoří nové pravidlo.

Změnit – upraví existující pravidlo.

Odstranit – odebere existující pravidlo.

Zobrazit předdefinovaná pravidla – pravidla předdefinovaná ESET Smart Security, která povolují nebo blokují definovanou komunikaci. Pravidla můžete deaktivovat, ale nemůžete je odstranit.

Nahoru/Výše/Dolů/Níže – umožní přizpůsobit pořadí vyhodnocování pravidel (vyhodnocovány jsou ze shora dolů).

4.3.3.2 Práce s pravidly

Změna pravidla je vyžadována vždy, když dojde ke změně sledovaných parametrů spojení. V takovém případě totiž pravidlo již nesplňuje podmínku a není tedy na něj uplatněna definovaná akce. V konečném důsledku to může znamenat zamítnutí spojení a následné problémy s funkčností aplikace. Příkladem je změna síťové adresy vzdálené strany nebo čísla portu.

Horní část okna pro změnu pravidla obsahuje tři záložky:

- **Obecné** – část, ve které zadáváte název pravidla, směr spojení, akci (**Povolit**, **Zakázat**, **Dotázat se**), protokol a profil, ve kterém se pravidlo použije,
- **Lokální strana** – zobrazuje informace o lokální straně spojení, včetně lokálního portu, rozsahu portů a komunikující aplikace. Přidat můžete také rozsah adres nebo zónu.
- **Vzdálená strana** – obsahuje informace o portu, respektive rozsahu vzdálených portů. Kromě toho umožňuje definovat také seznam vzdálených IP adres nebo zón, kterých se dané pravidlo týká. Přidat můžete také rozsah adres nebo zónu.

Při vytváření nového pravidla je potřeba zadat **Název pravidla**. Dále je nutné z rozbalovacího menu vybrat **Směr komunikace**, pro který bude pravidlo uplatněno a vybrat **akci**, která se provede při splnění podmínek pravidla.

Protokol představuje komunikační protokol, pro který bude pravidlo uplatňováno. Z rozbalovacího menu vyberte protokol, pro které má protokol platit.

Kód/Typ ICMP představuje ICMP zprávy identifikované číslem (například 0 reprezentuje "Echo Reply").

Všechna pravidla jsou standardně platná pro **Jakýkoli profil**. V případě potřeby můžete vybrat z rozbalovacího menu vybrat vlastní **Profil**.

Pokud zaškrtnete možnost **Zapsat do protokolu**, po uplatnění pravidla se zapíše událost do protokolu. Možnost **Upozornit uživatele** znamená, že při uplatnění pravidla se zobrazí uživateli bublina s informací o použití pravidla.

Příkladem přidání nového pravidla může být povolení prohlížeči webových stránek přistupovat k síti. Prohlížeči musí být umožněno následující:

- Na záložce **Obecné** povolena odchozí komunikace pomocí protokolu TCP & UDP,
- Na záložce **Lokální strana** přidán samotný soubor aplikace (v případě Internet Exploreru je to iexplore.exe),
- Na záložce **Vzdálená strana** je vhodné nastavit číslo portu 80, pokud chceme povolit přístup pouze k standardním webovým službám.

Poznámka: Mějte na paměti, že předefinovaná pravidla není možné měnit, pouze je můžete deaktivovat.

4.3.4 Jak nastavit zóny

Zóny představují síťové adresy, které dohromady tvoří jednu logickou skupinu. Na každou adresu dané skupiny se následně aplikují stejná pravidla definovaná pro celou skupinu. Tyto zóny můžete spravovat v **Rozšířeném nastavení** > **Personální firewall** > **Obecné**, po kliknutí na tlačítko **Změnit** vedle položky **Zóny**. Pro vytvoření nové zóny klikněte na tlačítko **Přidat**, zadejte její **Název**, **Popis** a přidejte vzdálenou IP adresu do pole **Vzdálená adresa počítače (IPv4/IPv6, rozsah, maska)**.

V dialogovém okně **Zóny firewallu** můžete definovat název zóny, její popis a seznam adres. Pro více informace přejděte do kapitoly Editor známých sítí.

4.3.5 Známé sítě

Pokud počítač často připojujete k veřejným sítím nebo sítím mimo vaši pracovní síť, doporučujeme vám ověřit důvěryhodnost takových sítí. Po prvotním definování sítě, ESET Smart Security může rozpoznat důvěryhodnou síť na základě parametrů definovaných v sekci **Identifikace sítě**. To je užitečné pro počítače, které se připojují často do sítí s IP adresami podobnými důvěryhodné zóně. V některých případech, ESET Smart Security může prohlásit neznámou síť za důvěryhodnou. Pro eliminaci tohoto případu doporučujeme používat možnost **Autentifikace sítě**.

Po připojení počítače k síti nebo změně konfigurace sítě, ESET Smart Security prohledá seznam známých sítí, zda neobsahuje odpovídající záznam pro danou síť. V případě, že **Identifikace sítě** a **Autentifikace sítě** (nepovinné) bude vyhovovat záznamu, síť bude označená jako připojená. V případě, že nebude nalezena žádná známá síť, vytvoří se nová na základě zjištěné konfigurace sítě a standardně se pro ni použije přísný režim ochrany. Po připojení k takové síti se zároveň zobrazí dialog **Zjištěno připojení k nové síti**, pomocí kterého můžete nastavit režim ochrany v síti – **Domácí nebo firemní síť** / **Veřejná síť**. Pokud se připojíte k již známé síti, jejíž režim ochrany je nastaven na **Domácí nebo firemní síť**, všechny podsítě této sítě budou přidány do důvěryhodné zóny.

Poznámka: Pokud zaškrtnete možnost **Automaticky označovat nové sítě jako veřejné**, dialog **Zjištěno připojení k nové síti** se nezobrazí a síť bude automaticky označena jako veřejná. To znamená, že z takové sítě nebudou dostupné běžné funkce (například sdílení souborů nebo vzdálená plocha).

Známé sítě můžete konfigurovat ručně pomocí Editoru známých sítí.

4.3.5.1 Editor známých sítí

Seznam známých sítí můžete konfigurovat ručně po kliknutí na **Změnit** v **Rozšířeném nastavením** (dostupném po stisknutí klávesy **F5** v hlavním okně programu) > **Personální firewall** v sekci **Známé sítě**.

Sloupce

Název – název známé sítě.

Typ ochrany – zobrazuje jednu z těchto možností: **Domácí nebo firemní síť** nebo **Veřejná síť**.

Profil firewallu – zobrazuje profil, jaký bude uplatňován na komunikaci v dané síti.

Ovládací prvky

Přidat – přidá novou známou síť.

Změnit – upraví existující známou síť.

Odstranit – odebere existující známou síť.

Nahoru/Výše/Dolů/Níže – umožní přizpůsobit pořadí vyhodnocování známých sítí (vyhodnocovány jsou ze shora dolů).

Dialogové okno s konfigurací známé sítě je rozděleno do tří záložek:

Síť

V této sekci můžete definovat název sítě typ její ochrany (**Domácí nebo firemní síť** nebo **Veřejná síť**). Pomocí rozbalovacího menu **Profil firewallu** vyberte požadovaný profil pro tuto síť. Pokud nastavíte režim ochrany na **Domácí nebo firemní síť**, všechny připojené podsítě budou považovány za důvěryhodné. Například, pokud je síťový adaptér připojen k sítě s IP adresou 192.168.1.5 a maskou 255.255.255.0, podsíť 192.168.1.0/24 bude přidána do důvěryhodné zóny. Pokud má adaptér více adres/podsítí, všechny budou považovány za důvěryhodné, bez ohledu na nastavení **Identifikace sítě**.

Další adresy zadané do pole **Další důvěryhodné adresy** budou vždy přidány do důvěryhodné zóny adaptéru připojeného do této sítě (bez ohledu na režim ochrany sítě).

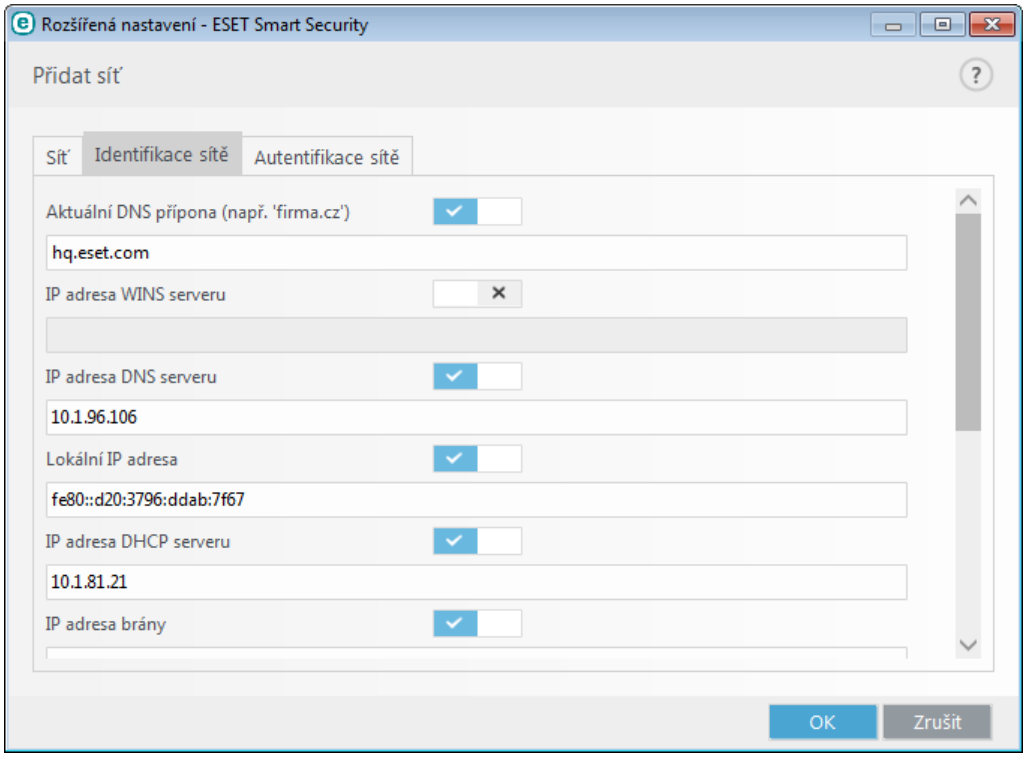
Následující parametry je nutné splnit, aby mohla být označená jako připojená v seznamu připojených sítí:

- Identifikace sítě – všechny vyplněné parametry musí odpovídat parametrům aktivního připojení.
- Autentifikace sítě – pokud je vybrán autentifikační server, musí dojít k úspěšnému ověření vůči ESET Authentication Serveru.

- Omezení sítě (pouze Windows XP/2003) – všechny vybrané globální omezení musí být vyplněny.

Identifikace sítě

Identifikace sítě probíhá na základě parametrů adaptéru lokální sítě. Identifikace je úspěšná, pokud definované parametry odpovídají aktivnímu připojení do sítě. Podporovány jsou IPv4 i IPv6 adresy.

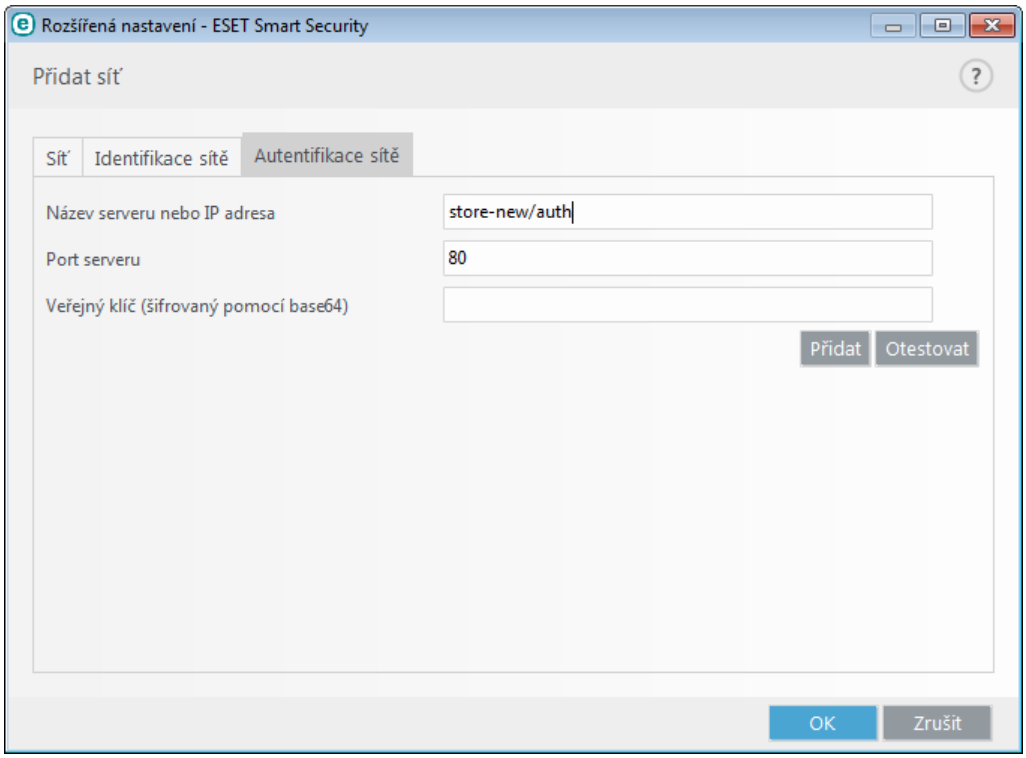


Autentifikace sítě

Autentifikace zóny vyhledává v síti specifický server a pro vlastní autentifikaci vůči serveru používá asymetrické šifrování (RSA). Název autentifikované sítě musí být odpovídat názvu sítě definovaném v nastavení autentifikačního serveru. Zadejte název serveru, naslouchající port a veřejný klíč, který odpovídá soukromému klíči serveru (více v kapitole Autentifikace sítě – konfigurace serveru). Název serveru musíte zadat ve formátu IP adresy, DNS nebo NetBios názvu. Za názvem serveru může následovat cesta upřesňující umístění klíče na serveru (např. *jméno_serveru/složka1/složka2/autentifikace*). Také můžete zadat více serverů, oddělených středníkem.

Zdroj, ze kterého se bude načítán veřejný klíč, může být soubor typu:

- PEM kryptovaný veřejný klíč (.pem). Tento klíč je možné vygenerovat prostřednictvím ESET Authentication Serveru (více v kapitole Autentifikace sítě – konfigurace serveru).
- Šifrovaný veřejný klíč
- Certifikát s veřejným klíčem (.crt)



Pro ověření nastavení klikněte na tlačítko **Otestovat**. V případě úspěšné autentizace se zobrazí oznámení *Autentifikace proběhla úspěšně*. Pokud není konfigurace správně nastavena, zobrazí se některé z následujících chybových hlášení:

Autentifikace k serveru nebyla úspěšná. Neplatný nebo neodpovídající podpis.
Podpis serveru neodpovídá zadanému veřejnému klíči.

Autentifikace k serveru nebyla úspěšná. Název sítě neodpovídá.
Název zóny na klientovi se neshoduje s názvem zóny nastavené na autentifikačním serveru. Je nutné, aby zóny byly pojmenovány stejně.

Autentifikace k serveru nebyla úspěšná. Neplatná nebo žádná odpověď od serveru.
Žádná odpověď, server neběží nebo není dostupný. Neplatnou odpověď můžete obdržet, pokud na dané adrese běží jiný HTTP server.

Zadaný veřejný klíč je neplatný.
Ověřte, že je veřejný klíč zadán správně.

Omezení sítě (pouze na Windows XP)

Moderní operační systémy (Windows Vista a novější), mohou mít pro každý síťový adaptér definovanou vlastní důvěryhodnou zónu, stejně tak profil firewallu. Bohužel tento koncept není podporován na Windows XP, proto všechny síťové adaptéry sdílejí stejnou důvěryhodnou zónu a aktivní profil firewallu. Jedná se o potenciální bezpečnostní riziko ve chvíli, kdy se počítač připojí zároveň k více sítím. V takovém případě může být komunikace z nedůvěryhodné zóny vyhodnocována důvěryhodnou zónu a profilem firewallu konfigurovaného pro jinou síť. Pro eliminaci tohoto bezpečnostního rizika můžete použít následující omezení a zabránit tak použití globální konfigurace na jinou (potenciálně nedůvěryhodnou) připojenou síť.

Na Windows XP se nastavení připojené sítě (důvěryhodná zóna a profil firewallu) aplikuje globálně, pokud je aktivní alespoň jedno z následujících omezení:

a. Je aktivní pouze jedno připojení
b. Není navázáno žádné bezdrátové připojení
c. Není navázáno žádné nezabezpečené bezdrátové připojení

4.3.5.2 Autentifikace zóny – nastavení serverové části

Autentifikace může být spuštěna na libovolném počítači/serveru připojeném do sítě, která má být autentifikována. Aplikace ESET Authentication Server musí být na počítači/serveru nainstalována a běžet, aby bylo možné provést autentifikaci kdykoliv při pokusu o připojení klienta do sítě. Instalační soubor aplikace ESET Authentication Server je možné stáhnout z webových stránek společnosti ESET.

Po nainstalování ESET Authentication Server se zobrazí hlavní okno autentifikačního serveru, které je možné později kdykoli vyvolat ručně přes nabídku **Start** > **Programy** > **ESET** > **ESET Authentication Server.**

Konfigurace autentifikačního serveru spočívá v zadání názvu autentifikační zóny, definování portu na kterém bude server naslouchat (standardně 80) a vygenerování soukromého a veřejného klíče, pomocí kterých bude autentifikace probíhat. Soukromý klíč zůstává na autentifikačním serveru, veřejný klíč je potřeba vložit na klientské straně do nastavení zón Personálního firewallu.

4.3.6 Protokolování

ESET Smart Security Personální firewall ukládá důležité události do protokolu, který je možné prohlížet přímo v hlavním okně po kliknutí na záložku **Nástroje** > **Další nástroje** > **Protokoly** a vybráním možnosti **Personální firewall** z rozbalovacího menu.

Poznámka: Pro aktivaci diagnostického protokolování personálního firewallu přejděte do **Rozšířeného nastavení** na záložku **Nástroje** > **Diagnostika** a vyberte možnost **Aktivovat diagnostické protokolování firewallu**. Následně se do protokolu zapíší všechna zablokovaná spojení.

Protokolování představuje účinný nástroj při odhalování chyb a zjišťování průniků do systému. Záznamy v protokolu ESET Personálního firewallu obsahují následující údaje:

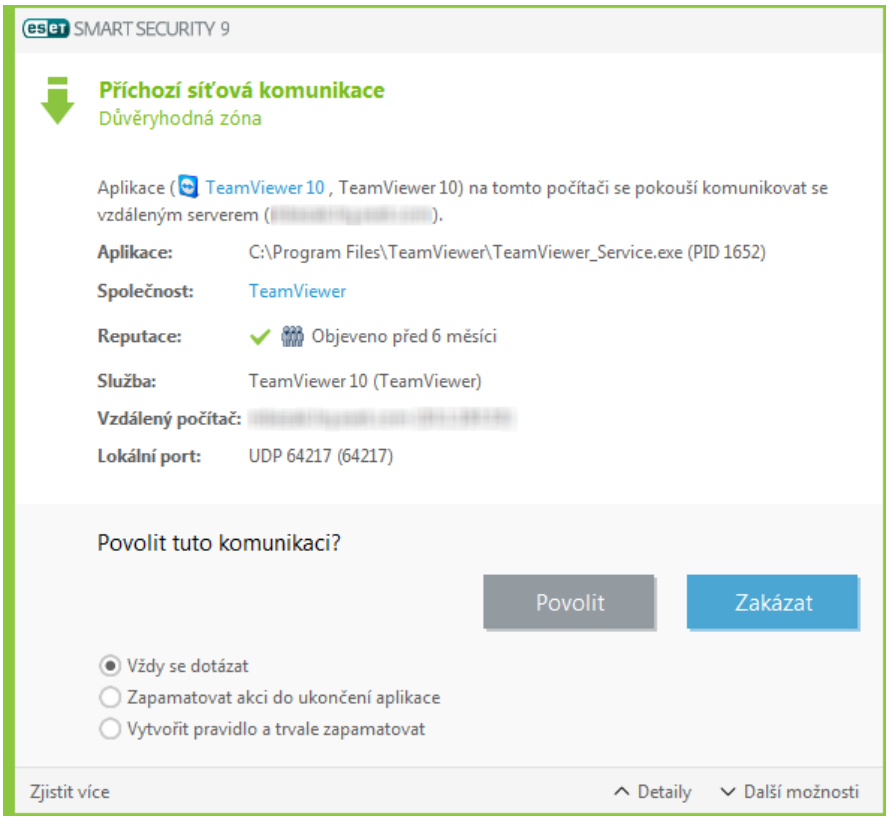
- **Čas** – datum a čas, kdy událost nastala,
- **Událost** – název události,
- **Zdroj** – zdrojovou síťovou adresu,
- **Cíl** – cílovou síťovou adresu,
- **Protokol** – protokol síťové komunikace,
- **Název pravidla/červa** – aplikované pravidlo, resp. název červa, pokud je identifikován,
- **Aplikace** – název komunikující aplikace,
- **Uživatel** – jméno uživatele.

Analyzováním těchto údajů můžete odhalit pokusy o narušení bezpečnosti systému. Příliš časté spojení z různých neznámých lokalit, hromadné pokusy o navázání spojení, komunikující neznámé aplikace či neobvyklá čísla portů mohou pomoci v odhalení potenciálního bezpečnostního rizika a minimalizaci jeho následků.

4.3.7 Navazování spojení – detekce

Personální firewall detekuje každé nově vzniklé síťové spojení. Podle nastavení režimu filtrování závisí, jaké činnosti pro toto nové spojení provede. Pokud je aktivován **Automatický** nebo **Administrátorský režim**, Personální firewall provede předem určené akce bez interakce uživatele.

V případě interaktivního režimu je zobrazeno informační okno, oznamující detekci nového síťového spojení spolu s informacemi a tomto spojení. Dané spojení můžete povolit nebo zablokovat. Pokud opakovaně povolujete stejné spojení, doporučujeme pro něj vytvořit pravidlo. To můžete provést zaškrtnutím možnosti **Zapamatovat si akci (vytvořit pravidlo)**, kdy se akce vytvoří jako nové pravidlo Personálního firewallu. Pokud firewall v budoucnu rozpozná stejné spojení, pravidlo se automaticky aplikuje bez nutnosti interakce uživatele.



Při zjištění neznámého spojení je potřeba postupovat obezřetně a povolovat pouze spojení, které jsou bezpečná. Personální firewall při povolení všech spojení ztrácí svůj význam. Důležitými parametry spojení jsou zejména:

- **Vzdálená strana** – povolujete pouze spojení na důvěryhodné a známé adresy,
- **Lokální aplikace** – není vhodné povolit spojení neznámým aplikacím a procesům,
- **Číslo portu** – komunikace na známých portech (např. HTTP komunikace – port číslo 80) je obvykle bezpečná.

Počítačové infiltrace pro své šíření ve velké míře využívají internet a skrytá spojení, pomocí kterých jsou schopné infikovat systém. Správnou konfigurací pravidel Personálního firewallu je možné ochránit systém před proniknutím škodlivého kódu.

4.3.8 Řešením problémů s ESET Personálním firewallem

Pokud se po instalaci ESET Smart Security potýkáte s problémy s připojením k internetu / síťovým prostředkům, existuje několik způsobů jak zjistit, zda problémy s připojením nezpůsobil ESET Personální firewall. Pokud ano, pomůže vám vytvořit nové pravidlo nebo výjimku pro vyřešení problémů s připojením.

V následujících kapitolách naleznete možné řešení problémů způsobené ESET Personálním firewallem:

- Průvodce řešením problémů
- Protokolování a vytváření pravidel nebo výjimek z protokolu
- Vytváření výjimek z oznámení Personálního firewallu
- Rozšířený PCAP protokol
- Řešení problémů s filtrováním protokolů

4.3.8.1 Průvodce řešením problémů

Průvodce řešením problémů má přehled o všech zablokovaných spojeních a provede vás výběrem zablokované aplikace nebo zařízení. Následně vám navrhne vytvoření sady pravidel, pro vyřešení problému. **Průvodce řešením problémů** naleznete v hlavním okně programu na záložce **Nastavení** > **Ochrana sítě**.

4.3.8.2 Protokolování a vytváření pravidel nebo výjimek z protokolu

Standardně ESET Personální firewall nezaznamenává všechna zablokovaná spojení. Pro zobrazení spojení zablokovaných ESET Personálním firewallem je nutné v **Rozšířeném nastavení** (dostupném po stisknutí **klávesy F5** v hlavním menu programu) v sekci **Nástroje** > **Diagnostika** zapnout možnost **Aktivovat diagnostické protokolování firewallu**. Pokud v protokolu naleznete spojení, které nechcete blokovat, stačí na něj kliknout pravým tlačítkem myši a z kontextového menu vybráním možnosti **Příště neblokovat podobné události** vytvořit IDS výjimku. Prosím, mějte na paměti, že protokol všech zablokovaných spojení může obsahovat stovky záznamů a může být obtížné najít v něm konkrétní komunikaci. Po vyřešení problému s komunikací nezapomeňte protokolování opět deaktivovat.

Pro více informací přejděte do kapitoly Protokoly.

Poznámka: Protokolování můžete použít pro zjištění pořadí pravidel, ve kterých ESET Personální firewall blokuje konkrétní spojení. Navíc z protokolu je možné vytvořit pravidlo přesně tak, jak jej potřebujete.

4.3.8.2.1 Vytváření výjimek z oznámení Personálního firewallu

Poté, co ESET Personální firewall detekuje škodlivou síťovou aktivitu, zobrazí na pracovní ploše upozornění s popisem události. Toto oznámení obsahuje odkaz, pomocí kterého si můžete zobrazit podrobnější informace o zablokované hrozbě a zároveň umožňuje vytvořit výjimku pro danou událost.

Poznámka: Pokud síťová aplikace nebo zařízení nesprávně implementuje síťové standardy, její komunikace může být odchycena modulem IDS. V takovém případě můžete přímo ze zobrazeného oznámení vytvořit v ESET Personálním firewallu výjimkou pro takovou aplikaci nebo zařízení.

4.3.8.3 Vytvoření pravidla z protokolu

V nové verzi ESET Smart Security můžete pravidla vytvářet přímo z protokolu. V hlavním okně programu přejděte na záložku **Nástroje** > **Další nástroje** > **Protokoly** a z rozbalovacího menu vyberte možnost **Personální firewall**. Následně klikněte pravým tlačítkem myši na požadovaný záznam a z kontextového menu vyberte možnost **Příště neblokovat podobné události**. Zobrazí se oznámení s informací, že bylo vytvořeno pravidlo.

Abyste mohli vytvářet pravidla z protokolu, je nutné v ESET Smart Security provést následující nastavení:

- nastavte v **Rozšířeném nastavení** (dostupném po stisknutí **klávesy F5** v hlavním okně programu) > **Nástroje** > **Protokoly** úroveň protokolování na získávání **Diagnostických záznamů**,
- aktivujte v **Rozšířeném nastavení** (dostupném po stisknutí **klávesy F5** v hlavním okně programu) > **Personální firewall** > **IDS a rozšířená nastavení** > **Detekce útoků** možnost **Zobrazit upozornění při pokusu o zneužití bezpečnostních děr**.

4.3.8.4 Rozšířený PCAP protokol

Tato funkce poskytne ESET technické podpoře podrobnější informace o síťové komunikaci povolené/zablokované ESET Personálním firewallem. Tuto funkci aktivujte pouze na výzvu specialisty technické podpory. Mějte na paměti, že následně se začne generovat velké množství dat a může dojít ke zpomalení počítače.

1. Otevřete **Rozšířené nastavení** > **Nástroje** > **Diagnostika** a zaškrtněte možnost **Aktivovat diagnostické protokolování firewallu**.
2. Pokuste se znovu navodit problém.
3. Deaktivujte rozšířené protokolování.
4. PCAP protokol naleznete ve stejné složce jako diagnostické výpisy:

- Microsoft Vista a novější

C:\ProgramData\ESET\ESET Endpoint Security\Diagnostics

- Microsoft XP/2003

  C:\Documents and Settings\All Users\ESET Endpoint Security\Diagnostics

4.3.8.5 Řešení problémů s filtrováním protokolů

Pokud pozorujete problémy při používání internetového prohlížeče nebo poštovního klienta, v prvním kroku doporučujeme ověřit, zda problém nezpůsobuje filtrování protokolů. Dočasně tedy v Rozšířeném nastavení deaktivujte filtrování protokolů (pokud se situace nezmění, nezapomeňte filtrování opět zapnout). Pokud problém po vypnutí filtrování zmizí, níže uvádíme seznam nejčastějším problémů a jejich řešení:

Problémy s aktualizací nebo zabezpečeným spojením

Pokud se aplikace nedokáže aktualizovat nebo komunikační kanál není zabezpečený:

- Pokud máte aktivní filtrování protokolu SSL, zkuste jej dočasně vypnout. V případě, že to pomůže, ponechte filtrování protokolu SSL aktivní a vytvořte výjimku na problematickou komunikaci:
  Přepněte filtrování protokolu SSL do interaktivního režimu. Znovu proveďte aktualizaci. Zobrazí se dialogové okno s informací o šifrované komunikaci. Ujistěte se, že komunikující aplikace je skutečně ta, která nefunguje a detailně prozkoumejte certifikát serveru. Následně vyberte možnost zapamatovat akci pro tento certifikát nebo klikněte na tlačítko Ignorovat. Pokud se již nezobrazí žádná další dialogová okna související s filtrování protokolu SSL, přepněte režim filtrování zpět na automatický. Tím by měl být problém vyřešen.
- Pokud se nejedná o internetový prohlížeč nebo poštovní klient, můžete danou komunikaci kompletně vyloučit z filtrování protokolu (pokud toto provede v případě internetového prohlížeče nebo poštovního klienta, budete vystaveni riziku). Všechny aplikace, jejichž komunikace již byla v minulosti filtrována by se měly zobrazit v seznamu aplikací, ve kterém je můžete vyloučit z filtrování protokolů.

Problémy s přístupem k síti

Pokud nejste schopni provádět žádné operace se síťovým zařízením (například zobrazit webovou stránku NAS nebo přehrávat video na domácím přehrávači), zkuste přidat IPv4 a IPv6 adresy na seznam vyloučených adres.

Problémy s konkrétní webovou stránkou

V tomto případě můžete pomocí správy adres vyloučit konkrétní webovou stránku z filtrování protokolů. Například, pokud nemáte přístup k https://www.gmail.com/intl/en/mail/help/about.html, zkuste přidat *gmail.com* do seznamu adres vyloučených z filtrování.

Chyba: "Některé podporované aplikace pro import kořenového certifikátu stále běží“

Pokud máte aktivní filtrování protokolu SSL, ESET Smart Security musí pro správnou funkci naimportovat certifikát do kořenového umístění aplikací využívajících SSL komunikaci. To není možné za jejich běhu. V tomto případě se jedná o internetový prohlížeč Firefox a Opera. Ujistěte se tedy, že neběží žádný internetový prohlížeč (nejlépe pohledem do Správce procesů, zda se v něm na záložce Procesy nenachází proces firefox.exe, thunderbird.exe nebo opera.exe) a zkuste to znovu.

Neplatný vydavatel nebo podpis certifikátu

V tomto případě se import certifikátu nezdařil. Nejprve se ujistěte, zda cílová aplikace neběží. Následně deaktivujte filtrování protokolu SSL a znovu jej aktivujte. Poté by již mělo dojít ke korektnímu importování.

4.4 Bezpečnostní nástroje

V sekci **Bezpečnostní nástroje** můžete zapnout nebo vypnout následující součásti:

- Ochrana bankovnictví a online plateb
- Rodičovská kontrola
- Anti-Theft

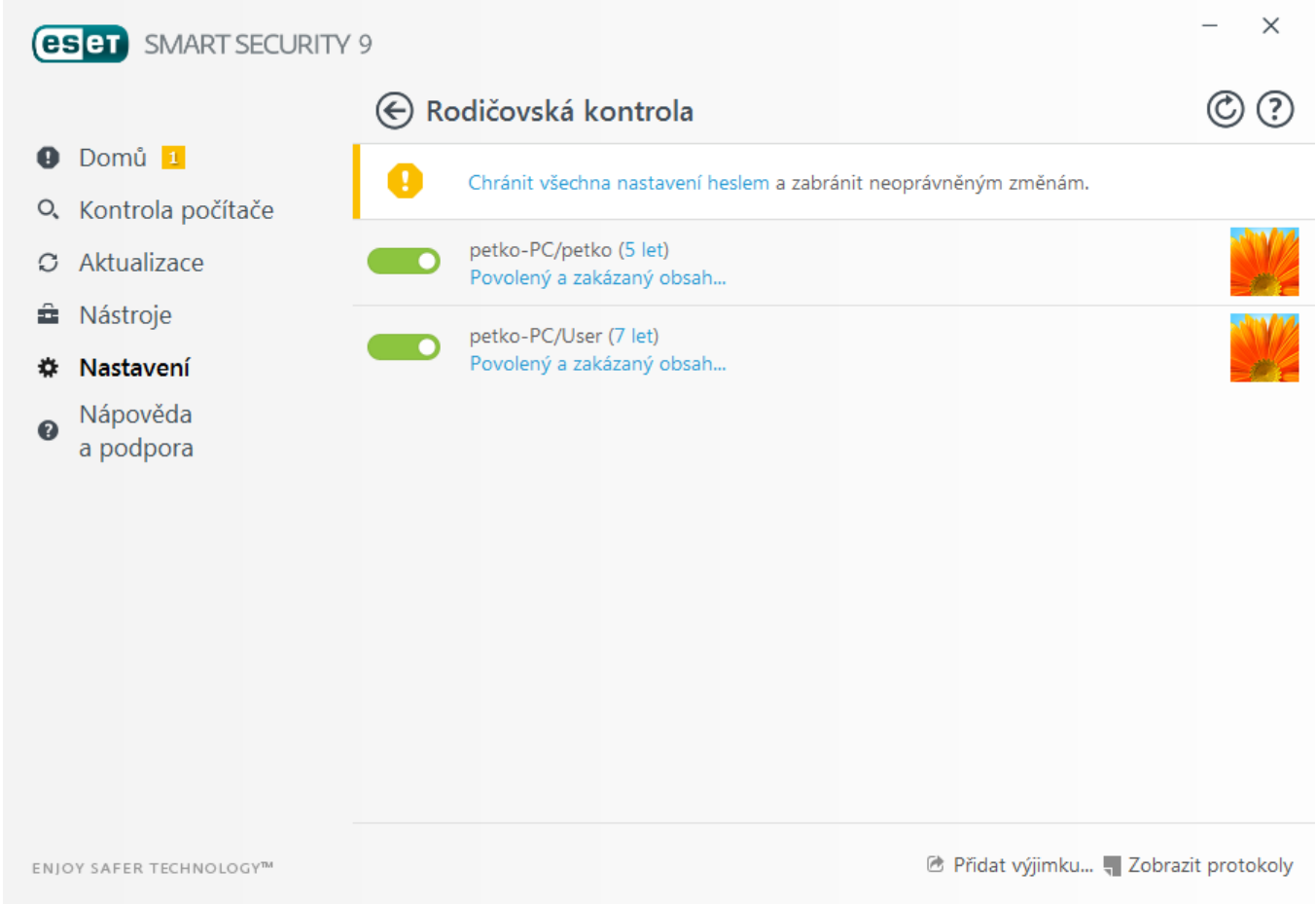
4.4.1 Rodičovská kontrola

V sekci **Rodičovská kontrola** můžete konfigurovat nastavení rodičovské kontroly, které vám umožňuje chránit vaše děti a nastavit omezení pro používání zařízení a služeb. Cílem je zabránit dětem, dospívajícím a zaměstnancům přístup na stránky s nevhodným nebo škodlivým obsahem.

Rodičovská kontrola umožňuje blokovat webové stránky, které mohou obsahovat nevhodný obsah. Kromě toho jako rodiče můžete zakázat přístup na 40 předdefinovaných kategorií webových stránek, které jsou dále rozděleny na více než 140 podkategorií.

Pro aktivování Rodičovské kontroly pro vybraný uživatelský účet postupujte podle následujících kroků.

1. V základním nastavení je Rodičovská kontrola vypnuta. Zapnout ji můžete dvěma způsoby:
   - Pomocí přepínače na záložce **Nastavení** > **Bezpečnostní nástroje** aktivujte rodičovskou kontrolu.
   - V hlavním okně programu stiskněte **klávesu F5** pro zobrazení Rozšířeného nastavení. V levé části klikněte na **Web a mail** > **Rodičovská kontrola** a v pravé části zaškrtněte možnost **Zapnout rodičovskou kontrolu**.
2. Klikněte na záložku **Nastavení** > **Bezpečnostní nástroje** > **Rodičovská kontrola** v hlavním okně programu. Přesto, že je funkce aktivována, musíte definovat uživatelské účty, pro které se má použít. To provedete kliknutím na možnost **Ochránit tento účet**. V nastavení účtu vyberte věk, který odpovídá danému uživateli, podle něhož se stanovuje úroveň filtrování webových stránek. Nyní bude Rodičovská kontrola aktivní pro vybraný uživatelský účet. Dále klikněte na možnost **Povolený a zakázaný obsah...** a přejděte na záložku Filtrování obsahu webu pro přizpůsobení kategorií stránek, které chcete povolit nebo blokovat. Pro blokování konkrétních stránek přejděte na záložku Blokované a povolené webové stránky.



Na záložce **Nastavení** > **Bezpečnostní nástroje** > **Rodičovská kontrola** jsou dostupné tyto možnosti:

Uživatelské účty Windows

V této části se zobrazí uživatelské účty ve Windows. Pomocí přepínačů a zapnete nebo vypnete rodičovskou kontrolu pro konkrétní uživatelský účet. Pod aktivním účtem najdete možnost Povolený a zakázaný obsah..., která slouží pro konfiguraci seznamu povolených kategorií, blokovaných a povolených stránek.

Důležité: Pro vytvoření nového účtu (např. pro dítě) postupujte podle následujících kroků (platí pro Windows 7 nebo Windows Vista):

1. Otevřete správce uživatelských účtů kliknutím na tlačítko **Start** (v levém dolním rohu obrazovky), vyberte **Ovládací panely** a poté **Uživatelské účty**.
2. Klikněte na **Spravovat další účet**. Pokud jste vyzváni k potvrzení, vyplňte příslušné údaje.
3. Klikněte na **Vytvořit nový účet**.
4. Pojmenujte účet a klikněte na **Vytvořit účet**.
5. Vraťte se do hlavního okna ESET Smart Security a přejděte na záložku **Nastavení** > **Bezpečnostní nástroje** > **Rodičovská kontrola**.

Odkazy v dolní části okna

Přidat výjimku... – po kliknutí přidáte snadno a rychle stránku, kterou chcete povolit nebo naopak blokovat.

Zobrazit protokol – zobrazí podrobný protokol o činnosti rodičovské kontroly (blokované stránky, účet pro který byla stránka zablokována, důvod zablokování, atd.). Také můžete tento protokol **Filtrovat...** podle požadovaných kritérií.

Doplňující informace

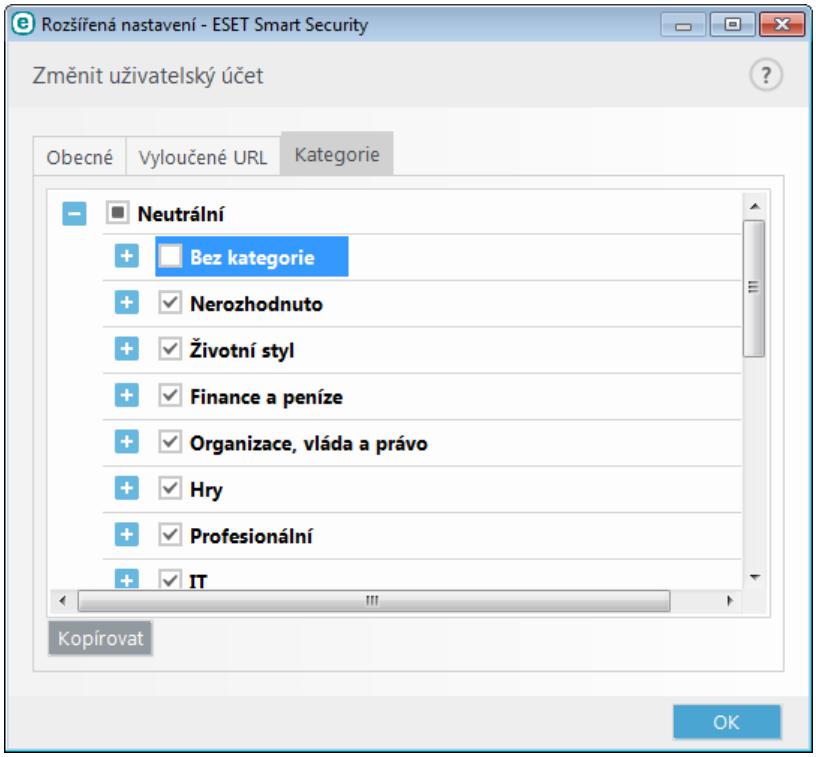
Je důležité chránit heslem nastavení programu ESET Smart Security. Toto heslo můžete nastavit v sekci Přístup k nastavení. Pokud není nastaveno žádné heslo pro ochranu nastavení, pod možností **Rodičovská kontrola** se zobrazí varování – Ochraňte nastavení heslem a zabraňte neoprávněným změnám. – a zobrazí se tlačítko **Nastavit heslo...**. Omezení nastavené v rodičovské kontrole ovlivní pouze standardní uživatelské účty, protože administrátor může kdykoli tato nastavení obejít.

Komunikace HTTPs (SSL) není v základním nastavení filtrována. Proto **Rodičovská kontrola** nemůže filtrovat stánky, které začínají *https://*. Zapnout kontrolu SSL můžete v **Rozšířeném nastavení** > **Web a mail** > **Kontrola protokolu SSL/TLS**, kde vyberete možnost **Zapnout filtrování protokolu SSL/TLS**.

Poznámka: Pro správné fungování Rodičovské kontroly je důležité, aby byla zapnutá také Kontrola aplikačních protokolů, Kontrola protokolu HTTP a Integrace Personálního firewallu do systému. Všechny tyto funkce jsou standardně zapnuté.

4.4.1.1 Kategorie

V tomto dialogovém okně vybíráte kategorie webových stránek, které chcete povolit nebo zakázat.

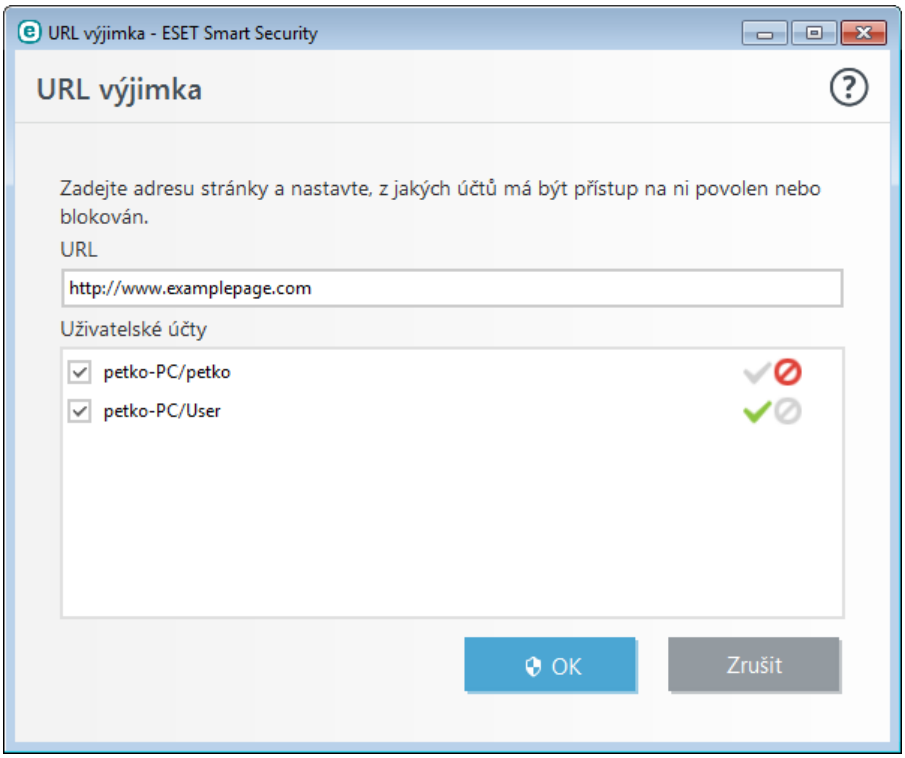


Po najetí myši na kategorii se zobrazí seznam stránek, které daná kategorie obsahuje. Níže jsou uvedeny příklady kategorií, jejichž obsah nemusí být na první pohled zřejmý.

- **Různé** – obvykle lokální adresy intranetu, 127.0.0.0/8, 192.168.0.0/16, atd. Pokud stránka hlásí kód chyby 403 nebo 404, pak také patří do této kategorie.
- **Nevyřešeno** – tato kategorie obsahuje stránky, o kterých nelze rozhodnout z důvodu připojení do databáze rodičovské kontroly.
- **Nezařazeno** – neznámé stránky nezařazené do databáze rodičovské kontroly.
- **Proxy servery** – anonymizéry, přesměrovače nebo veřejné proxy servery používané pro přístup k webovým stránkám, které jsou obvykle Rodičovskou kontrolou zakázány.
- **Sdílení souborů** – stránky, které obsahují velké množství dat například fotografie, videa nebo e-knihy. Takové stránky mohou potenciálně obsahovat škodlivý či nevhodný obsah.

4.4.1.2 Blokované a povolené webové stránky

Zadejte URL adresu do prázdného pole v dialogovém okně, vyberte akci **Povolit** nebo **Blokovat** a klikněte na **Přidat** pro zařazení adresy do seznamu. Pro vymazání URL adresy ze seznamu, vyberte požadovanou adresu a klikněte na tlačítko .



V seznamech URL adres není možné používat speciální znaky * (hvězdička) a ? (otazník). Adresy s více TLD musíte zadat ručně (webstranka.com, webstranka.sk atd.). Pokud vložíte adresu domény do seznamu, veškerý obsah nacházející se na této doméně a všechny její subdomény (např. sub.webstranka.com) budou blokovány nebo povoleny – podle toho, jakou akci jste pro URL adresy vybrali.

Poznámka: Blokování nebo povolení specifické internetové stránky může být přesnější než blokování nebo povolení celé kategorie internetových stránek. Při změně těchto nastavení buďte opatrní.

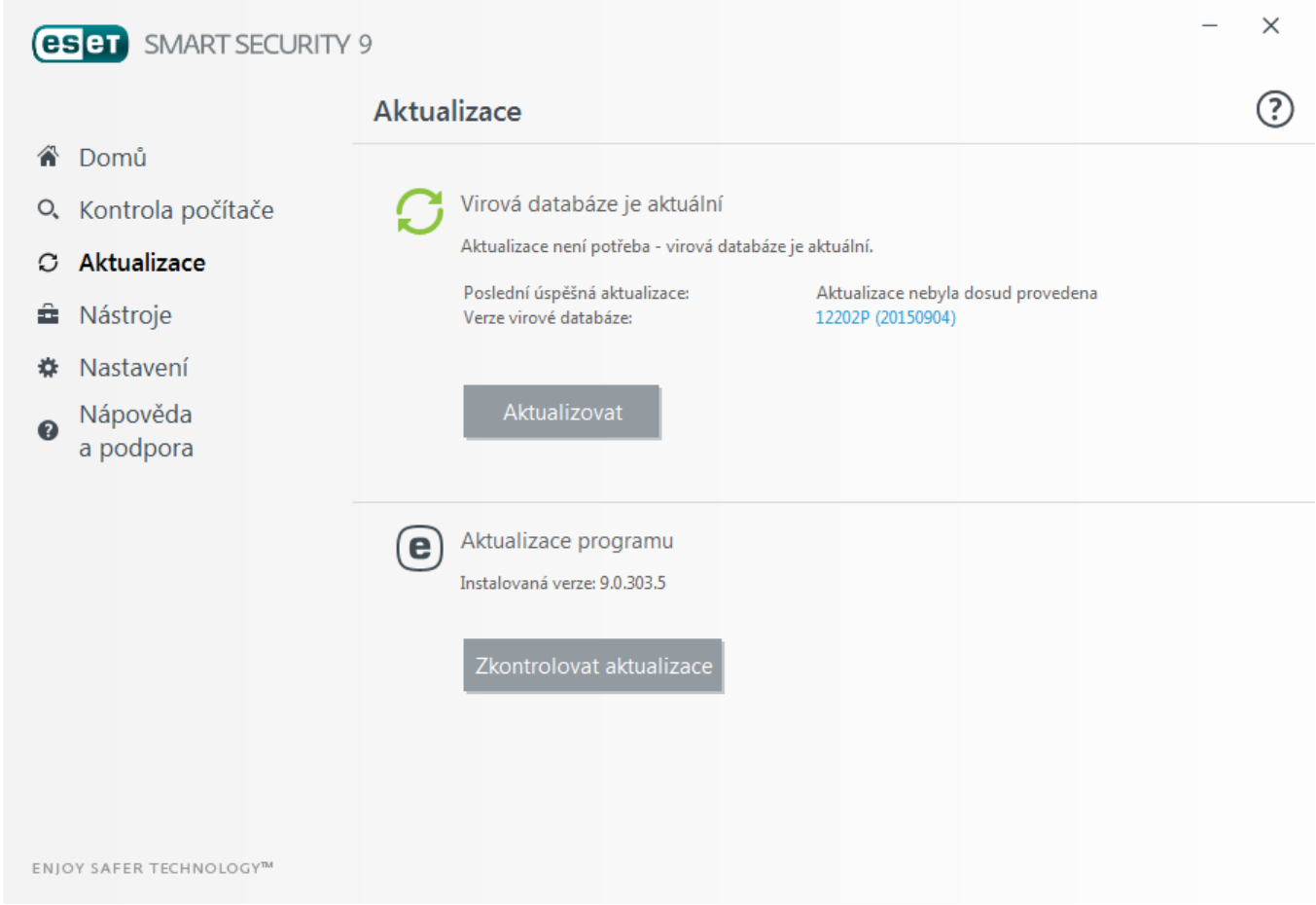
4.5 Aktualizace programu

Pravidelná aktualizace ESET Smart Security je základním předpokladem pro zajištění maximální bezpečnosti systému. Modul Aktualizace se stará o to, aby byl program stále aktuální pomocí aktualizace virové databáze stejně jako aktualizováním jednotlivých programových komponent.

Informace o aktuálním stavu aktualizace jsou zobrazovány na záložce **Aktualizace** v hlavním okně programu. Obsahuje informaci o datu a čase poslední úspěšné aktualizace, zda je virová databáze aktuální, případně jestli není potřeba program aktualizovat. Číselné označení verze virové databáze je funkční odkaz vedoucí na webové stránky společnosti ESET s podrobnými informacemi o nových vzorcích, které aktualizace zahrnuje.

Aktualizace se kontrolují, stahují a instalují automaticky, ale můžete ověřit dostupnost aktualizací kdykoli kliknutím na tlačítko **Aktualizovat**. Pro správnou funkčnost programu a ochranu proti škodlivému software je nezbytné aktualizovat virovou databázi a programové komponenty. Věnujte pozornost konfiguraci a průběhu aktualizací. Pokud jste produkt do této chvíle neaktivovali, budete k tomu vyzváni. Po kliknutí na tlačítko **Aktivovat produkt** zadejte licenční klíč.

Poznámka: Licenční klíč jste obdrželi po nákupu nebo registraci ESET Smart Security.

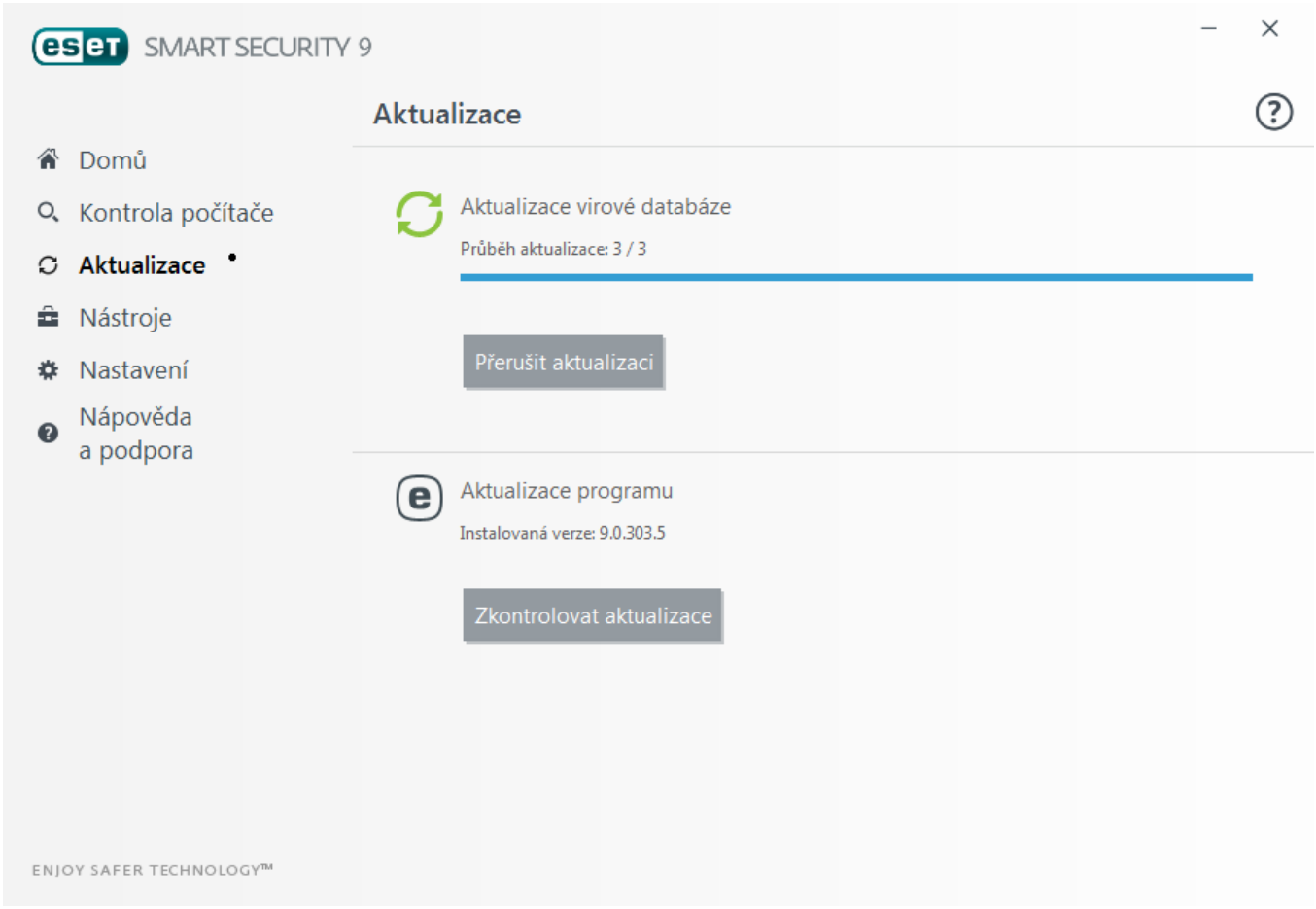


Poslední úspěšná aktualizace – zobrazuje datum, kdy se program naposledy aktualizoval. Pokud nevidíte dnešní datum, virová databáze nemusí být aktuální.

Verze virové databáze – zobrazuje číslo verze virové databáze. Číslování určuje výrobce a číslo poslední verze je možné najít na internetových stránkách společnosti ESET.

Průběh stahování

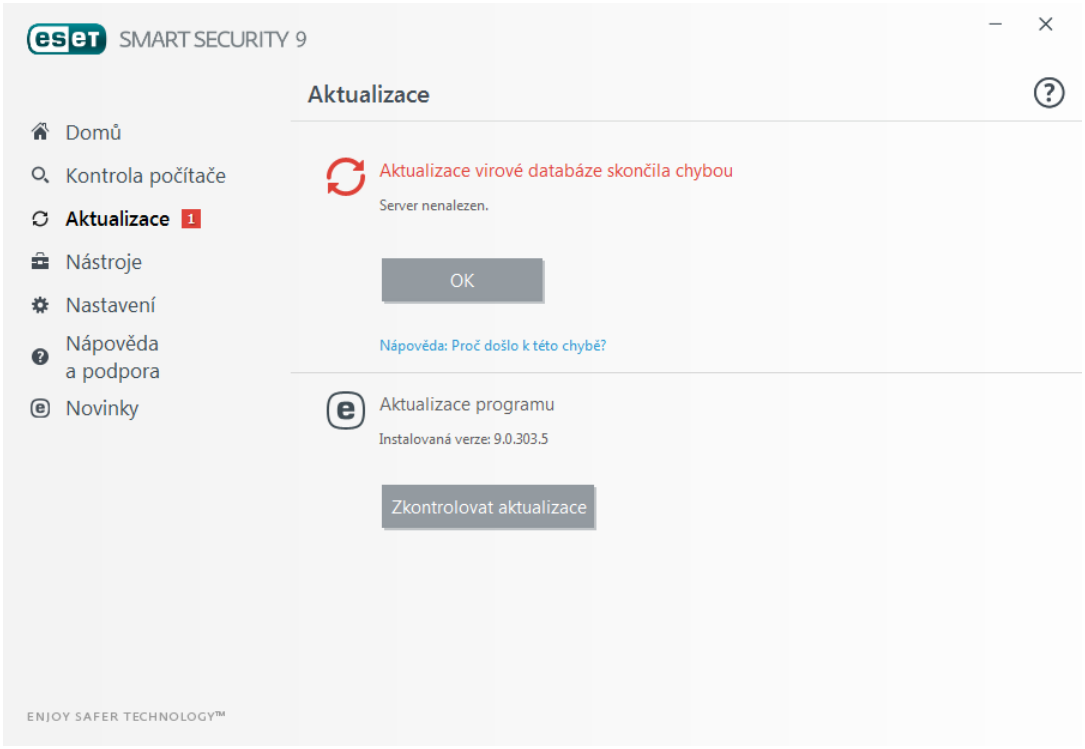
Po kliknutí na tlačítko **Aktualizovat** se spustí proces stahování. Zároveň se zobrazí průběh stahování souboru aktualizace a zbývající čas do konce. Kliknutím na tlačítko **Přerušit** se aktualizace zastaví.



Důležité: Za normálních okolností, při pravidelné a úspěšném stahování aktualizací, se v okně **Aktualizace** zobrazuje zpráva: **Aktualizace není potřeba - virová databáze je aktuální**. Pokud tomu tak není, program není aktualizován a zvyšuje se riziko infiltrace. V takovém případě doporučujeme co nejdříve aktualizovat virovou databázi.

V některých případech se může zobrazit chybová zpráva **Aktualizace virové databáze skončila chybou**, a to z níže uvedených důvodů:

1. **Program není aktivován/Neplatná licence** – v hlavním okně program přejděte na záložku **Nápověda a podpora**, kde klikněte na tlačítko **Správa licence**. Poté vyberte způsob aktivace a postupujte podle kroků na obrazovce.
2. **Chyba při stahování souborů aktualizace** – při pokusu o stažení souboru aktualizace došlo k chybě. Chyba může souviset s nesprávným nastavením připojení k internetu. Doporučujeme zkontrolovat připojení k internetu (otevřením jakékoliv webové stránky ve webovém prohlížeči). Rovněž doporučujeme zkontrolovat, zda je počítač připojen k internetu, a ověřit, zda poskytovatel internetu nemá výpadek připojení.



Poznámka: Pro více informací přejděte do ESET Databáze znalostí.

4.5.1 Nastavení aktualizace

Možnosti aktualizace jsou dostupné v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu) na záložce **Aktualizace** > **Obecné**. Nastavení aktualizace se skládá ze zadání zdroje aktualizace, tedy z nastavení aktualizačních serverů a autentifikace vůči těmto serverům

Profil

Aktuálně používaný aktualizační profil se zobrazuje v rozbalovacím menu **Aktivní profil**. Pro vytvoření nového nebo úpravu již existujícího klikněte na **Změnit** vedle položky **Seznam profilů**.

Většinu problémů souvisejících s aktualizací virové databáze vyřešíte vymazáním aktualizační cache po kliknutí na tlačítko **Vyčistit**.

Upozornění na zastaralou virovou databázi

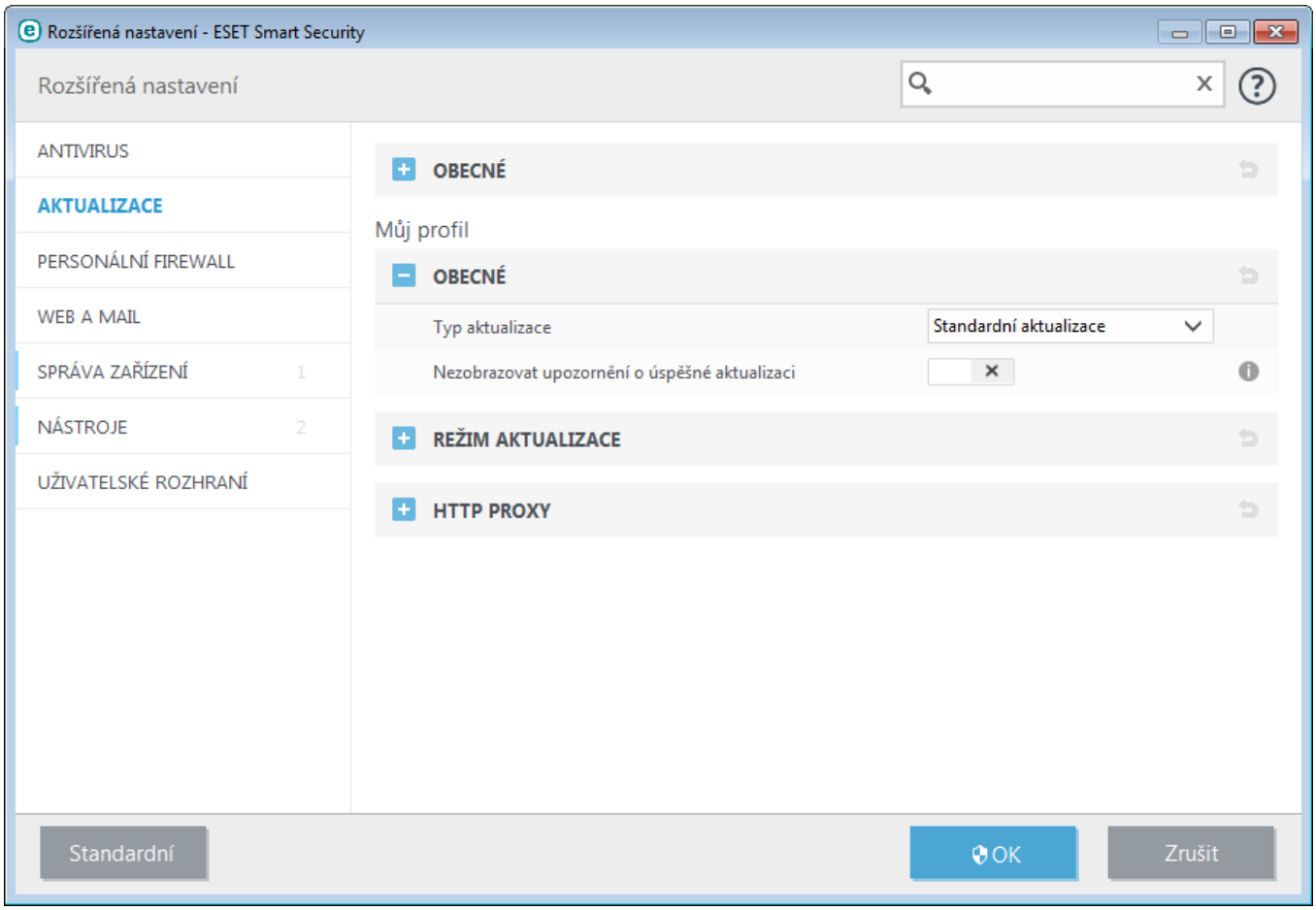
Nastavit automaticky maximální stáří databáze – pomocí této možnosti nastavíte maximální přístupné stáří virové databáze. Bude-li databáze starší, zobrazí se informace, že je virová databáze zastaralá. Předdefinovaná doporučená hodnota je 7 dní.

Vrátit předchozí aktualizace

Pokud máte podezření, že nová aktualizace virové databáze je nestabilní nebo poškozená, můžete vrátit virovou databázi do předchozího stavu a na stanovený časový interval zakázat aktualizace.

ESET Smart Security zálohuje virovou databázi a jednotlivé programové moduly pro případ obnovení starší verze. Aby se obrazy tzv. snapshoty virové databáze vytvářely, ponechte možnost **Vytvářet zálohu aktualizačních souborů** zaškrtnutou. **Počet vytvářených záloh** určuje počet obrazů předchozích virových databází uložených na lokálním disku počítače

Pokud kliknete na Vrátit předchozí aktualizaci (**Rozšířená nastavení** (F5) > **Aktualizace** > **Vrátit předchozí aktualizace**), je potřeba z rozbalovacího menu **Pozastavit aktualizace** vybrat interval, který určuje, na jak dlouho bude aktualizace virové databáze a programových modulů pozastavena.



Pro správné fungování aktualizace je nezbytné zadat veškeré aktualizační informace správně. Pokud používáte firewall, ujistěte se, že má produkt ESET povolenou HTTP komunikaci.

Obecné

Standardně jsou jako **Typ aktualizace** nastaveny vybrány **Standardní aktualizace**. Tím je zajištěno automatické stahování aktualizací ze serverů společnosti ESET. Pokud je vybrána možnost **Testovací aktualizace**, budou se při aktualizaci stahovat beta verze modulů a virové databáze. V předstihu tak získáte přístup k novějším funkcím, opravám a metodám detekce škodlivého kódu. Protože testovací aktualizace nereprezentují finální kvalitu, neměli byste je instalovat na produkční stroje a pracovní stanice, u který je vyžadována stabilita a dostupnost. Vyberete-li možnost **Opožděná aktualizace**, aktualizace se budou stahovat z aktualizačního severu, na který jsou aktualizace umisťovány se zpožděním (o několik hodin). Výhodou je stahování ověřených aktualizací, které nezpůsobují problémy, ale zároveň se tím snižuje úroveň zabezpečení.

Nezobrazovat upozornění o úspěšné aktualizaci – vypne zobrazování oznámení v pravém dolním rohu obrazovky. Použití této možnosti je užitečné v případě, kdy na počítači běží aplikace na celou obrazovku. Stejnou akci můžete nastavit pomocí Herního režimu.

4.5.1.1 Profily aktualizace

Aktualizační profily můžete použít pro různá nastavení aktualizací. Vytvoření aktualizačních profilů pro aktualizaci má význam především pro mobilní uživatele, kteří si mohou vytvořit alternativní profil pro internetové připojení, které se často mění.

V rozbalovacím menu **Aktivní profil** se vždy zobrazuje aktuálně vybraný profil. Standardně je vybrána možnost **Můj profil**. Vytvoření nového profilu je možné provést prostřednictvím tlačítka **Profily...** a dále přes tlačítko **Přidat...**., kde zadejte vlastní **Název profilu**. Při vytváření nového profilu můžete použít stávající nastavení pomocí možnosti **Kopírovat z nastavení profilu**.

V rámci nastavení profilu můžete pro každý profil vybrat odlišný aktualizační server, prostřednictvím kterého aktualizace proběhne, přičemž můžete vybrat existující ze seznamu serverů nebo přidat nový server. Seznam existujících aktualizačních serverů je dostupný v rozbalovacím menu **Aktualizační server**. Pro přidání nového serveru do seznamu klikněte na tlačítko **Upravit...** v sekci **Nastavení aktualizace** pro vybraný profil a následně klikněte na **Přidat**.

4.5.1.2 Pokročilá nastavení aktualizace

Pokročilé nastavení aktualizace zobrazíte kliknutím na tlačítko **Nastavit...**, kde můžete konfigurovat Režim aktualizace a HTTP Proxy.

4.5.1.2.1 Režim aktualizace

V sekci **Režim aktualizace** se nachází nastavení související s pravidelným stahováním aktualizací virové databáze a automatickou aktualizací programu na novou verzi.

Pokud aktivujete možnost **Aktualizovat aplikaci**, program bude pravidelně ověřovat dostupnost nové verze produktu a automaticky novou verzi nainstaluje. Aktualizace na novější verzi zpravidla nevyžaduje interakci uživatele, pouze je nutné restartovat počítače. Na nutnost restartování vás aplikace upozorní.

Pokud vyberete možnost **Dotázat se před stahováním aktualizací**, před stažením nové aktualizace se zobrazí informace, že je dostupná aktualizace. Následně bude nutné stažení aktualizace potvrdit.

V případě, že aktualizační soubor bude větší než definovaná hodnota pomocí možnosti **Dotázat se, pokud je velikost aktualizačního souboru větší než (kB)**, zobrazí informace, zda chcete aktualizaci stáhnout. Tato možnost je vhodná při mobilních připojení, kdy potřebujete šetřit množství přenášených dat.

4.5.1.2.2 HTTP Proxy

Pro přístup k nastavení proxy serveru pro daný aktualizační profil přejděte v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu) na záložku **Aktualizace** > **HTTP Proxy**. V rozbalovacím menu **Režim proxy** jsou dostupné následující možnosti:

- **Nepoužívat proxy server**,
- **Spojení pomocí proxy serveru,**
- **Použít globální nastavení proxy serveru.**

Vybráním možnosti **Použít globální nastavení proxy serveru** se použijí veškerá nastavení proxy serveru definovaná v Rozšířeném nastavení na záložce **Nástroje** > **Proxy server**.

Pomocí možnosti **Nepoužívat proxy server** zajistíte, aby se při aktualizaci ESET Smart Security nepoužíval proxy server.

Možnost **Spojení pomocí proxy serveru** vyberte v případě, že:

- Pro aktualizaci ESET Smart Security potřebujete použít jiné, než globální nastavení proxy serveru definované v Rozšířeném nastavení ve větvi **Nástroje** > **Proxy server**. Pokud vyberte tuto možnost, je potřeba zadat adresu **Proxy serveru**, komunikační **Port** a také **Uživatelské jméno** a **Heslo**,
- Nebylo definováno globální nastavení proxy serveru, ale pro aktualizaci ESET Smart Security se má používat proxy,
- Počítač je připojen k internetu pomocí proxy serveru a nastavení bylo v průběhu instalace programu převzato z

Internet Exploreru, ale v průběhu času došlo ke změně nastavení proxy serveru (například z důvodu přechodu k jinému poskytovatel internetu). V tomto případě doporučujeme zkontrolovat nastavení proxy zobrazené v tomto okně a případně jej změnit pro zajištění funkčnosti aktualizací.

Standardně je nastavena možnost **Použít globální nastavení proxy serveru**.

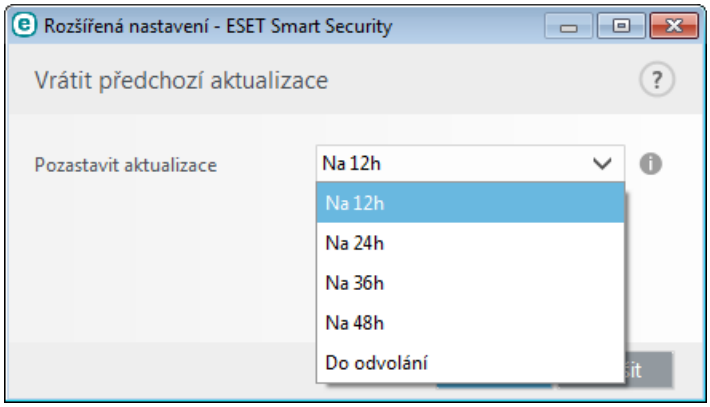
Poznámka: Autentifikační údaje jako **Uživatelské jméno** a **Heslo** pro proxy server se vyplňují v případě, že je proxy server vyžaduje. Mějte na paměti, že se nejedná o údaje, které jste obdrželi při koupi produktu ESET Smart Security

4.5.2 Vrátit předchozí aktualizace

Pokud máte podezření, že nová aktualizace virové databáze je nestabilní nebo poškozená, můžete vrátit virovou databázi do předchozího stavu a na stanovený časový interval pozastavit aktualizace.

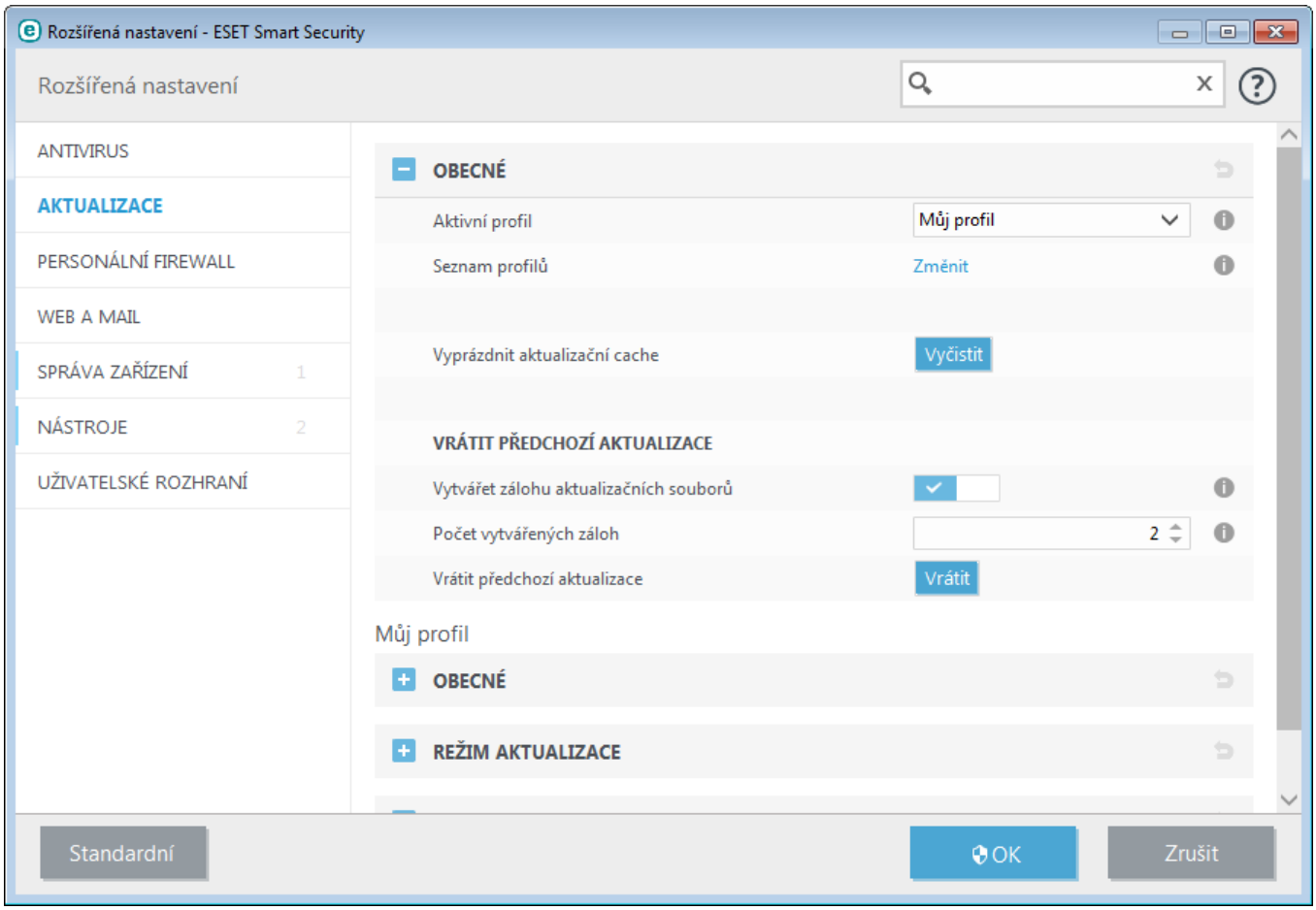
ESET Smart Security zálohuje virovou databázi a jednotlivé programové moduly pro případ obnovení starší verze. Aby se obrazy tzv. snapshoty virové databáze vytvářely, ponechte aktivní možnost **Vytvářet zálohu aktualizačních souborů**. **Počet záloh vytvářených lokálně** určuje počet obrazů předchozích virových databází uložených na lokálním disku počítače.

Pokud kliknete na tlačítko **Vrátit předchozí aktualizace** (v **Rozšířeném nastavení** (F5) > **Aktualizace**), je potřeba z rozbalovacího menu **Časový interval** vybrat interval, na jak dlouho chcete aktualizaci virové databáze a programových modulů pozastavit.



Vyberte možnost **Do odvolání**, pokud chcete funkci aktualizace obnovit ručně. Protože tato možnost představuje potenciální bezpečnostní riziko, její výběr nedoporučujeme.

Pro provedení této akce se obnoví nejstarší uložená virová databáze uložená v počítači a zároveň se text tlačítka změní na **Povolit aktualizace**.



Příklad: Nejnovější verze virové databáze má číslo 9556. Na pevném disku počítače jsou uloženy obrazy virových databází 9555 a 9553. Všimněte si, že verze 9554 není k dispozici, protože počítač byl například delší dobu vypnut, proto byla stažena novější verze databáze. Pokud jste jako **Počet záloh vytvářených lokálně** nastavili číslo 2, po navrácení změn se obnoví virová databáze (včetně programových modulů) s číslem 9553. Tento proces může chvíli trvat. Pro ověření, zda se vrátila předchozí verze virové databáze, přejděte v hlavním okně ESET Smart Security na záložku Aktualizace.

4.5.3 Jak vytvořit aktualizační úlohu

Aktualizaci můžete provést ručně kliknutím na tlačítko **Aktualizovat** na záložce **Aktualizace** v hlavním okně programu.

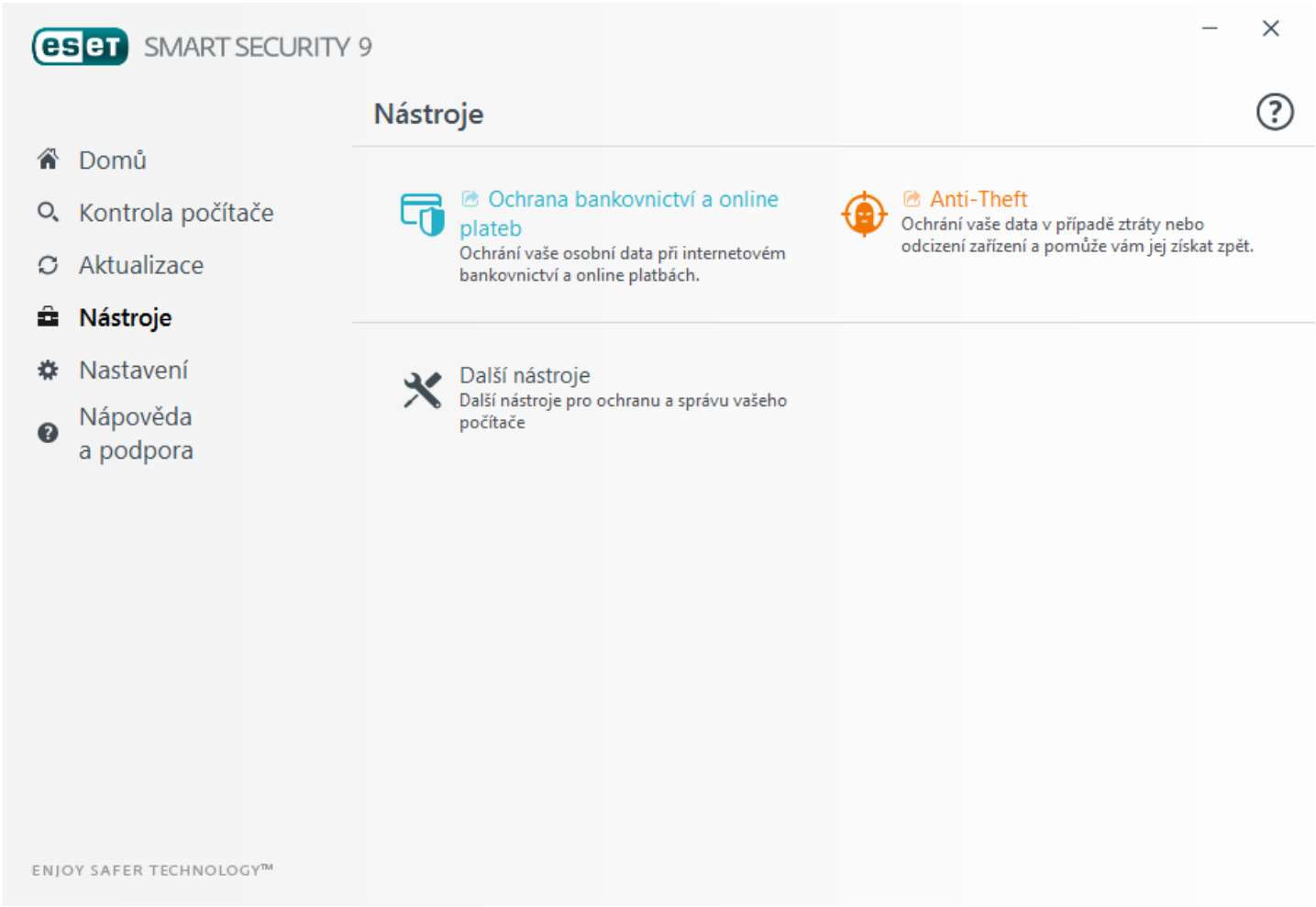
Aktualizaci můžete spouštět jako naplánovanou úlohu. Pro konfiguraci naplánované úlohy klikněte na záložku **Nástroje** > **Plánovač**. Standardně jsou po instalaci ESET Smart Security vytvořeny následující aktualizační úlohy:

- **Pravidelná automatická aktualizace**,
- **Automatická aktualizace po modemovém spojení**,
- **Automatická aktualizace po přihlášení uživatele**.

Každou z uvedených aktualizačních úloh můžete upravit podle svých představ. Kromě standardních aktualizačních úloh můžete vytvořit nové aktualizační úlohy s vlastním nastavením. Podrobněji se vytváření a nastavení aktualizačních úloh zabýváme v kapitole Plánovač.

4.6 Nástroje

Záložka **Nástroje** obsahuje součásti, které usnadňují správu programu a nabízejí rozšířené možnosti pro pokročilé uživatele.



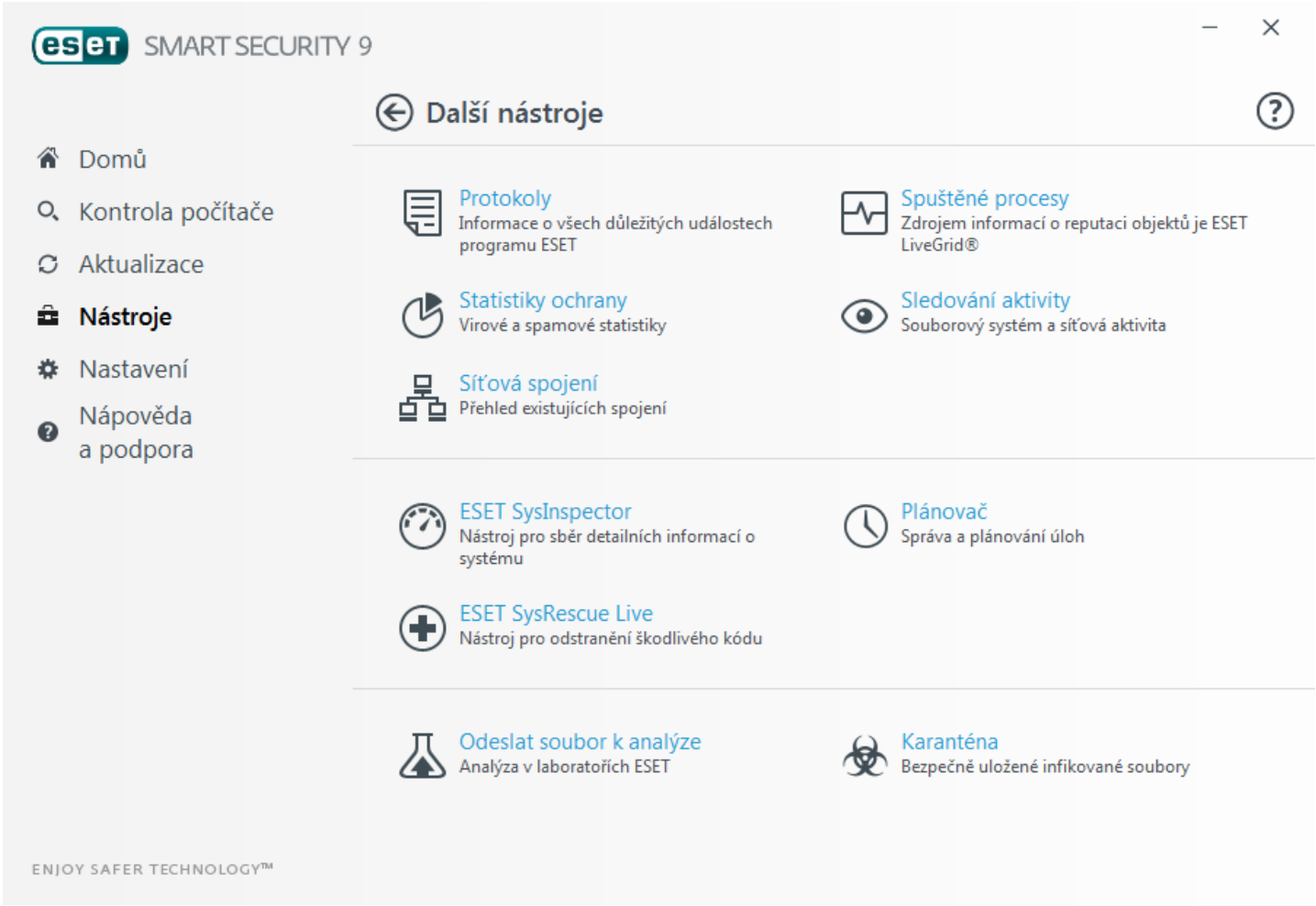
Ochrana bankovnictví a online plateb – ESET Smart Security dokáže ochránit vaše osobní data, čísla bankovních účtů a kreditních karet při používání online platbách prostřednictvím zabezpečeného prohlížeče. Pro více informací přejděte do této kapitoly.

Anti-Theft – ochrání vaše data v případě ztráty nebo odcizení zařízení a pomůže vám jej získat zpět. Pro více informací přejděte do této kapitoly.

Po kliknutí na možnost Další nástroje, si zobrazíte součásti pro zkušené uživatelé určené pro správu a diagnostiku produktu.

4.6.1 Nástroje produktu ESET Smart Security

V hlavním menu programu na záložce Nástroje > **Další nástroje** naleznete součásti určené pro zkušené uživatele, které vám usnadní správu a diagnostiku programu.



ESET Smart Security nabízí následující nástroje:

Protokoly

Statistiky ochrany

Sledování aktivity

Spuštěné procesy (tato součást je dostupná, pokud máte aktivní technologii ESET LiveGrid®)

Síťová spojení (tato součást je dostupná, pokud máte aktivní Personální firewall)

ESET SysInspector

ESET SysRescue Live – přesměruje vás na webové stránky společnosti ESET, kde si můžete stáhnout přímo obraz ESET SysRescue Live nebo nástroj pro vytvoření záchranného CD/USB..

Plánovač

Odeslat soubor k analýze – umožní odeslat podezřelý soubor k analýze do virové laboratoře ESET. Po kliknutí se zobrazí dialogové okno, které je popsané v kapitole Odeslání souboru k analýze.

Karanténa

4.6.1.1 Protokoly

Protokoly obsahují informace o všech důležitých událostech programu, které nastaly a poskytují přehled o detekovaných hrozbách. Protokolování představuje silný nástroj při systémové analýze, odhalování problémů a rizik a v neposlední řadě při hledání řešení. Zaznamenávání probíhá aktivně na pozadí bez jakékoli interakce s uživatelem a zaznamenávají se informace na základě nastavení citlivosti protokolování. Prohlížení textových zpráv a protokolů je možné přímo z prostředí ESET Smart Security a stejně tak je tyto protokoly možné archivovat.

Protokoly jsou přístupné v hlavním okně po kliknutí na záložku **Nástroje** > **Další nástroje** > **Protokoly**. Následně z rozbalovacího menu **Protokoly** vyberte požadovaný typ protokolu.

- **Zachycené hrozby** – protokol zachycených infiltrací poskytuje detailní informace týkající se infiltrací zachycených moduly ESET Smart Security. Informace zahrnují čas detekce, název infiltrace, umístění, provedenou činnost a uživatele přihlášeného v době detekce. Dvojklikem na záznam protokolu otevřete detaily v samostatném okně.
- **Události** – protokol událostí obsahuje informace o všech událostech ESET Smart Security a chybách, které se vyskytly. Informace z tohoto protokolu mohou pomoci najít příčiny problémů, případně jejich řešení.
- **Kontrola počítače** – protokol kontroly počítače obsahuje výsledky dokončené ruční nebo naplánované kontroly. Každý řádek náleží samostatné kontrole. Dvojklikem na záznam protokolu otevřete detaily v samostatném okně.
- **HIPS** – protokoly obsahují záznamy konkrétních pravidel, která se mají zaznamenávat. V protokolu je zobrazena aplikace, která danou operaci vyvolala, výsledek (tzn. zda bylo pravidlo povoleno, nebo zakázáno) a název vytvořeného pravidla
- **Personální firewall** – protokol obsahuje všechny vzdálené útoky zachycené personálním firewallem. Ve sloupci *Událost* se zobrazuje seznam útoků, ve sloupci *Zdroj* se zobrazují podrobnější informace o útočníkovi a ve sloupci *Protokol* naleznete komunikační protokol použitý při útoku. Analyzování tohoto protokolu pomůže včas odhalit pokusy o průnik do systému. Pro více informací o síťových útocích přejděte do kapitoly IDS a pokročilé možnosti.
- **Filtrované webové stránky** – tento seznam je užitečný v případě, že si chcete prohlédnout stránky blokované modulem Ochrana přístupu na web nebo Rodičovská kontrola. Protokol obsahuje informace o času, URL adrese, uživateli a aplikaci, která se chtěla na stránky připojit.
- **Antispamová ochrana** – obsahuje záznamy související s e-mailovými zprávami, které byly označeny jako spam.
- **Rodičovská kontrola** – protokol zobrazuje webové stránky, které byly zablokovány nebo povoleny. Sloupce *Typ vyhodnocení* a *Hodnota vyhodnocení* informují o tom, jakým způsobem byla pravidla filtrování aplikována.
- **Správa zařízení** – obsahuje záznamy o výměnných médiích nebo zařízeních připojených k počítači. V protokolu se zobrazí pouze zařízení, na která byla aplikována pravidla Správce zařízení. Pokud nebylo na zařízení aplikováno žádné pravidlo, záznam v protokolu se nevytvoří. Pro každé zařízení se zobrazí také informace o typu zařízení, sériové číslo, název výrobce a velikost média (pokud jsou dostupné).

V každé sekci můžete jednotlivé události kopírovat do schránky přímo po označení události a kliknutím na tlačítko **Kopírovat** (nebo pomocí klávesové zkratky **Ctrl + C**). Pro výběr více záznamů stiskněte zároveň klávesu **CTRL** nebo **SHIFT**.

Po kliknutí na přepínač **Filtrování** se zobrazí dialogové okno **Filtrování protokolu**, pomocí kterého můžete definovat kritéria filtrování.

V okně **Protokoly** můžete vyvolat kontextové menu kliknutím pravým tlačítkem myši na konkrétní záznam. Dostupné jsou následující možnosti:

- **Zobrazit** – zobrazí v novém okně všechny záznamy protokolu.
- **Filtrovat záznamy stejného typu** – po aktivovaní tohoto filtru se zobrazí pouze záznamy stejného typu (diagnostické, varování,...),
- **Filtrovat.../Hledat...** – po kliknutí se otevře dialogové okno Filtrování protokolu, ve kterém můžete definovat kritéria pro filtrování záznamů,
- **Zapnout filtr** – aktivuje filtr,
- **Zrušit filtr** – vypne filtrování a vymaže všechna kritéria pro filtrování (jak je popsáno výše),
- **Kopírovat/Kopírovat vše** – zkopíruje všechny záznamy z daného okna,
- **Odstranit/Odstranit vše** – odstraní vybrané/všechny záznamy – tato akce vyžaduje administrátorská oprávnění,
- **Exportovat...** – uloží vybrané záznamy do .XML formátu,
- **Exportovat vše...** – uloží všechny záznamy do .XML formátu,
- **Rolovat výpis protokolu** – pokud je tato možnost povolena, starší protokoly budou automaticky rolovat a v okně **Protokoly** se zobrazí pouze ty nejnovější.

4.6.1.1.1 Protokoly

Nastavení protokolování produktu ESET Smart Security je přístupné z hlavního okna programu. Přejděte na záložku **Nastavení** a klikněte na **Rozšířená nastavení** > **Nástroje** > **Protokoly**. V této sekci můžete upravit způsob správy protokolů. Program dokáže automaticky odstraňovat staré protokoly, čímž šetří místo na disku. V nastavení můžete vybrat následující možnosti:

Zaznamenávat události od úrovně – umožňuje nastavit úroveň, od které se budou zaznamenávat události do protokolu.

- **Diagnostické** – obsahují informace důležité pro ladění programu a všechny níže uvedené záznamy,
- **Informační** – obsahují informační zprávy, například o úspěšné aktualizaci a všechny níže uvedené záznamy,
- **Varování** – obsahují varovné zprávy a kritické chyby,
- **Chyby** – obsahují chyby typu "Chyba při stahování souboru aktualizace" a kritické chyby,
- **Kritické chyby** – obsahují pouze kritické chyby (chyba při startu antivirové ochrany, Personálního firewallu, atd...).

Poznámka: Všechna zablokovaná spojení se do protokolu zapíší při vybrání diagnostické úrovně.

Pomocí možnosti **Automaticky vymazat záznamy starší než (dní)** můžete nastavit po kolika dnech se záznamy mají vymazat.

Automaticky optimalizovat protokoly – zajistí automatickou defragmentaci protokolů, pokud počet nevyužitých záznamů překročí zadaný poměr v procentech v poli **Při překročení počtu nevyužitých záznamů (v procentech)**.

Kliknutím na **Optimalizovat** spustíte defragmentaci protokolů. Defragmentace odstraňuje prázdné záznamy v protokolech, čímž zvyšuje rychlost zpracovávání. Viditelné zlepšení práce s protokoly je po optimalizaci znatelné hlavně především u protokolů s velkým množstvím záznamů.

Pomocí možnosti **Zaznamenávat textové protokoly** aktivujete ukládání protokolů do odlišeného formátu:

- **Cílová složka** – složka, do které se uloží protokoly (pouze pro Text/CSV). Každý protokol se ukládá do samostatného souboru (například ve *virlog.txt* naleznete **Zachycené hrozby**, pokud protokoly ukládáte jako prostý text).

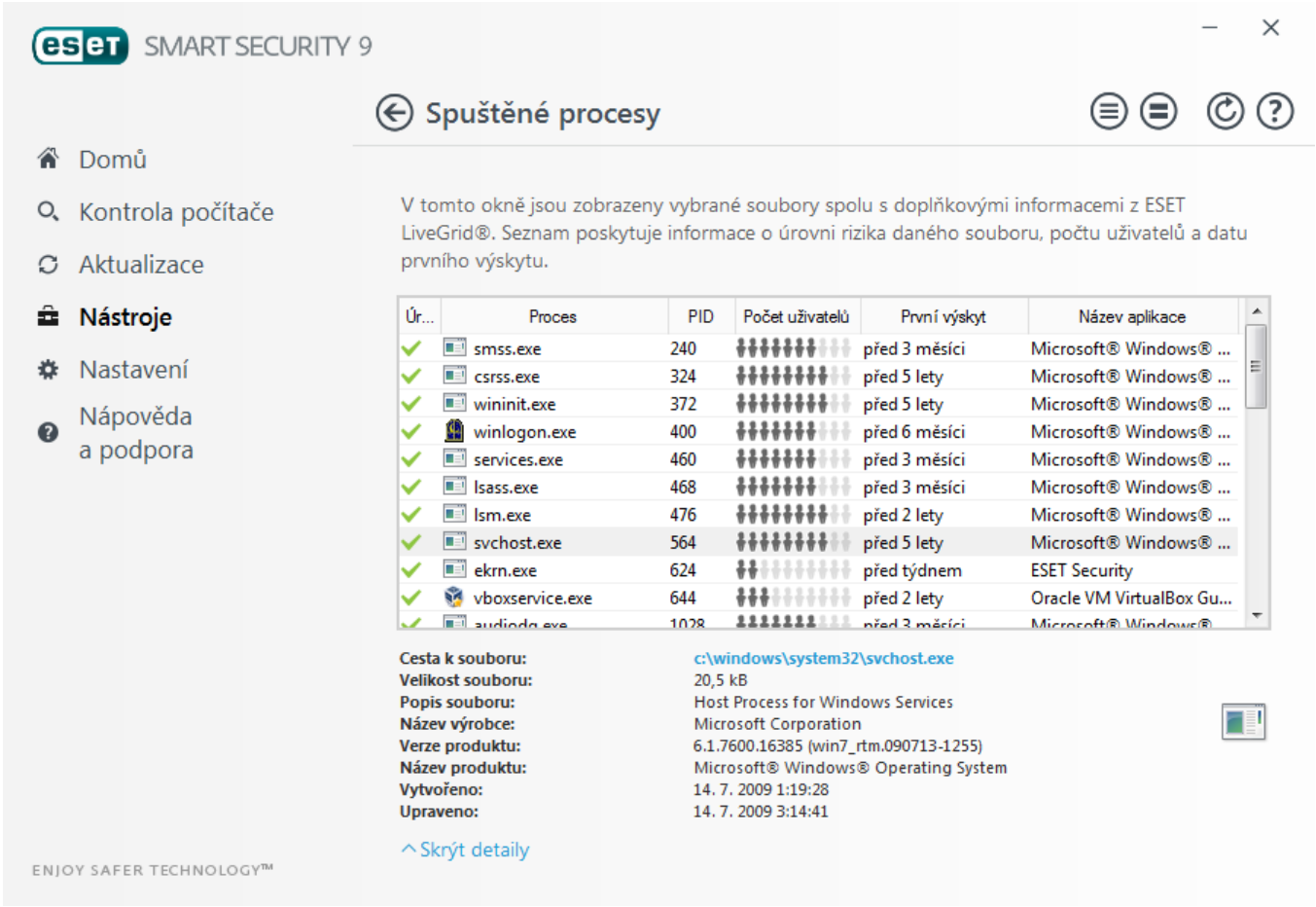
- **Typ** – pokud vybere **Text** jako formát souborů, protokoly budou uloženy do textového souboru; data budou oddělena tabulátorem. Stejný princip platí pro soubory oddělené středníkem **CSV**. Pokud vyberete **Událost**, protokol bude uložen do systémového Protokolu událostí, který si můžete zobrazit v Prohlížeči událostí.

Odstranit všechny protokoly – po kliknutí vymaže všechny protokoly vybrané v rozbalovacím menu **Typ**. O úspěšném vymazání protokolů budete informováni.

Poznámka: Specialisté technické podpory vás mohou požádat o zaslání protokolů, které mohou urychlit řešení vašeho problému. Pomocí nástroje ESET Log Collector snadno získáte diagnostické informace z počítače včetně protokolů. Pro více informací o používání tohoto nástroje navštivte ESET Databázi znalostí.

4.6.1.2 Spuštěné procesy

Tento nástroj zobrazuje spuštěné programy a procesy a umožňuje společnosti ESET získávat informace o nových infiltracích. ESET Smart Security poskytuje detailnější informace o spuštěných procesech díky technologii ThreatSense pro zajištění lepší ochrany uživatelů.



Úroveň rizika – ve většině případů přiřazuje ESET Smart Security objektům (souborům, procesům, klíčům registru apod.) úroveň rizika pomocí technologie ESET LiveGrid® na základě heuristických pravidel a kontroly každého objektu na přítomnost škodlivého kódu. Poté na základě těchto výsledků přidělí procesům úroveň rizika od 1 – V pořádku (zelený) až po 9 – Nebezpečný (červený).

Proces – název aplikace nebo procesu, který aktuálně běží na počítači. Pro zobrazení všech běžících programů na počítači můžete použít také Správce úloh systému Windows. Správce úloh spustíte kliknutím pravým tlačítkem na Hlavní panel a vybráním možnosti **Spustit správce úloh**, případně pomocí klávesové zkratky **Ctrl** + **Shift** + **Esc**.

PID – ID běžícího procesu v operačním systému Windows.

Poznámka: Aplikace označené jako 1 – V pořádku (zelený) jsou bezpečné a vyloučené z kontroly pro zajištění vyššího výkonu kontroly počítače.

Počet uživatelů – počet uživatelů, kteří používají danou aplikaci. Tyto informace se shromažďují pomocí technologie ESET LiveGrid®.

První výskyt – doba, kdy byl proces poprvé objeven pomocí technologie ESET LiveGrid® .

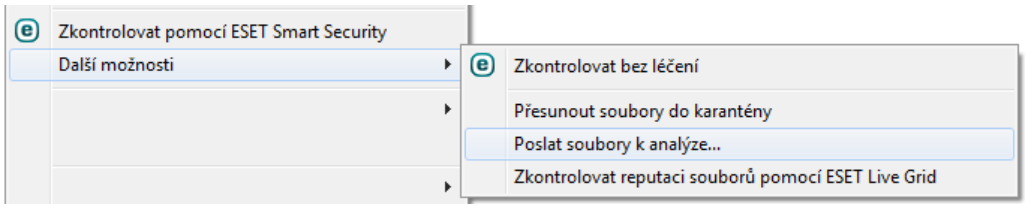
Poznámka: I v případě, že je aplikace označená jako Neznáma (oranžová), nemusí to nutně znamenat, že obsahuje škodlivý kód. Obvykle se jedná o novou aplikaci. Pokud si nejste jisti, zda je tomu opravdu tak, můžete soubor odeslat k analýze do virové laboratoře společnosti ESET. Pokud se potvrdí, že jde o aplikaci obsahující škodlivý kód, její detekce bude zahrnuta do další aktualizace.

Název aplikace – název aplikace nebo procesu.

Po kliknutí na konkrétní aplikaci a možnost **Zobrazit detaily** se v dolní části okna zobrazí následující informace:

- **Cesta k souboru** – umístění aplikace v počítači,
- **Velikost souboru** – velikost souboru v B (bajtech),
- **Popis souboru** – charakteristika souboru vycházející z jeho popisu získaného od operačního systému,
- **Název výrobce** – název výrobce aplikace nebo procesu,
- **Verze produktu** – tato informace pochází od výrobce aplikace nebo procesu,
- **Název produktu** – název aplikace, obvykle obchodní název produktu,
- **Vytvořeno** – datum a čas, kdy byla aplikace vytvořena,
- **Upraveno** – datum a čas, kdy byla aplikace naposledy upravena.

Poznámka: Reputace může být použita také u souborů, které se nechovají jako spuštěné programy/procesy – na soubor, který chcete zkontrolovat, klikněte pravým tlačítkem myši a ze zobrazeného kontextového menu vyberte **Další možnosti** > **Zkontrolovat reputaci souborů pomocí ESET LiveGrid®**.



4.6.1.3 Statistiky ochrany

Statistické údaje, které se týkají různých modulů ochrany programu ESET Smart Security jsou dostupné na záložce **Nástroje** > **Statistiky ochrany**. Pro zobrazení informací z požadovaných modulů použijte rozbalovací menu. Následně se ve spodní části okna zobrazí graf s legendou, která rovněž slouží jako filtr zobrazených položek. Po ponechání kurzoru na vybrané položce legendy se v grafu zobrazí pouze daná položka.

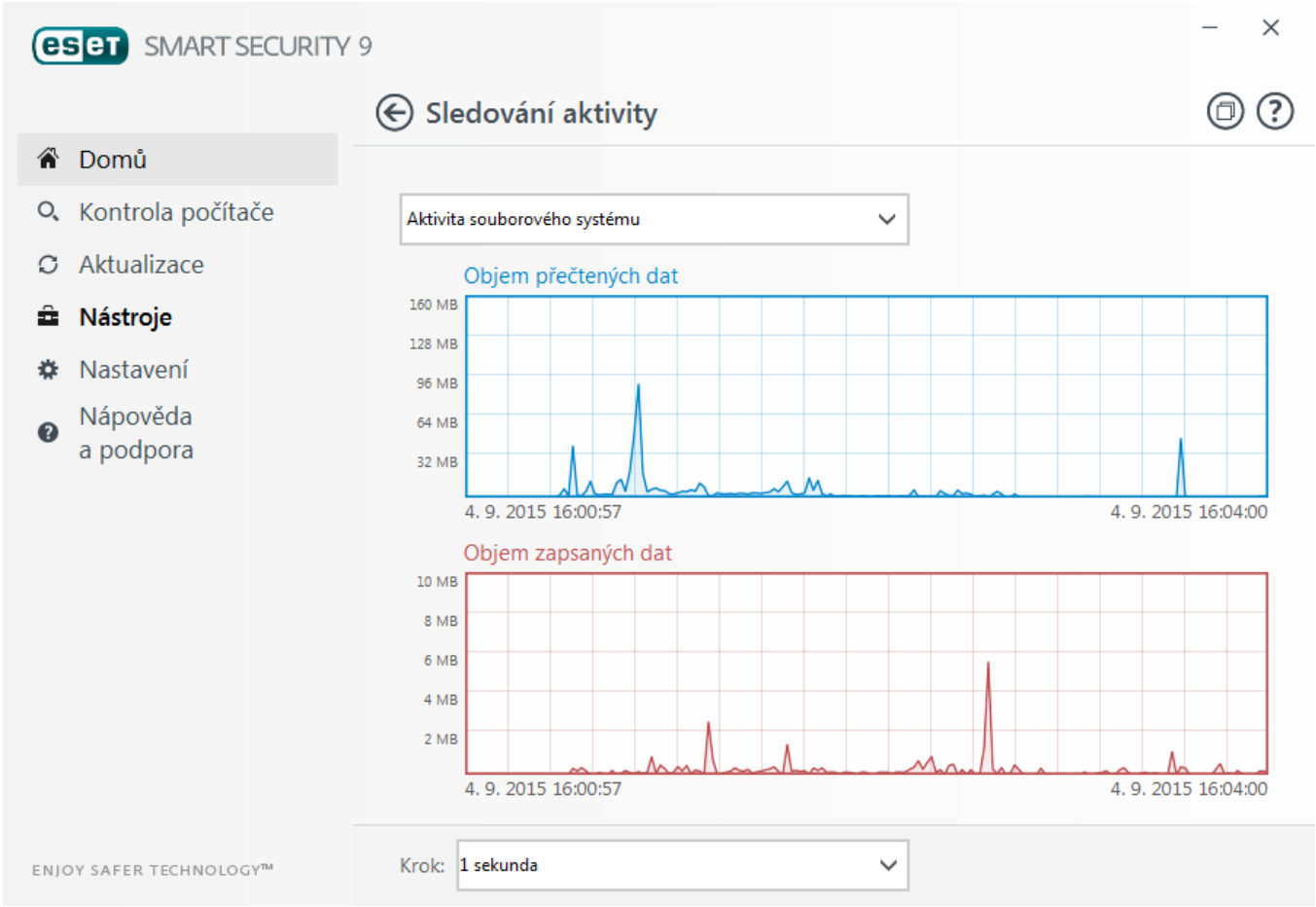
K dispozici jsou následující statistické informace:

- **Antivirová a antispywarová ochrana** – zahrnuje celkový počet infikovaných a vyléčených objektů,
- **Ochrana souborového systému** – zobrazí pouze objekty, které byly čteny nebo zapisovány na souborový systém,
- **Ochrana poštovních klientů** – zobrazí pouze objekty, které byly přijaty nebo odeslány pomocí poštovních klientů,
- **Ochrana přístupu na web** – zobrazí pouze objekty, které byly přijaty pomocí internetových prohlížečů,
- **Antispamová ochrana poštovních klientů** – zobrazí historii antispamu od posledního spuštění.

Pod grafem statistik se zobrazuje celkový počet kontrolovaných objektů, poslední kontrolovaný objekt a čas zahájení kontroly. Kliknutím na **Vynulovat statistiky** vynulujete veškeré statistické informace.

4.6.1.4 Sledování aktivity

Pro zjednodušené sledování činnosti systému je na záložce **Nástroje**> **Další nástroje** > **Sledování aktivity** k dispozici grafické rozhraní, které umožňuje v reálném čase sledovat aktivitu souborového systému. Ve spodní části se zobrazuje časová osa, jejíž měřítko můžete změnit pomocí kontextového menu **Krok**.



K dispozici jsou následující rozlišení měřítka:

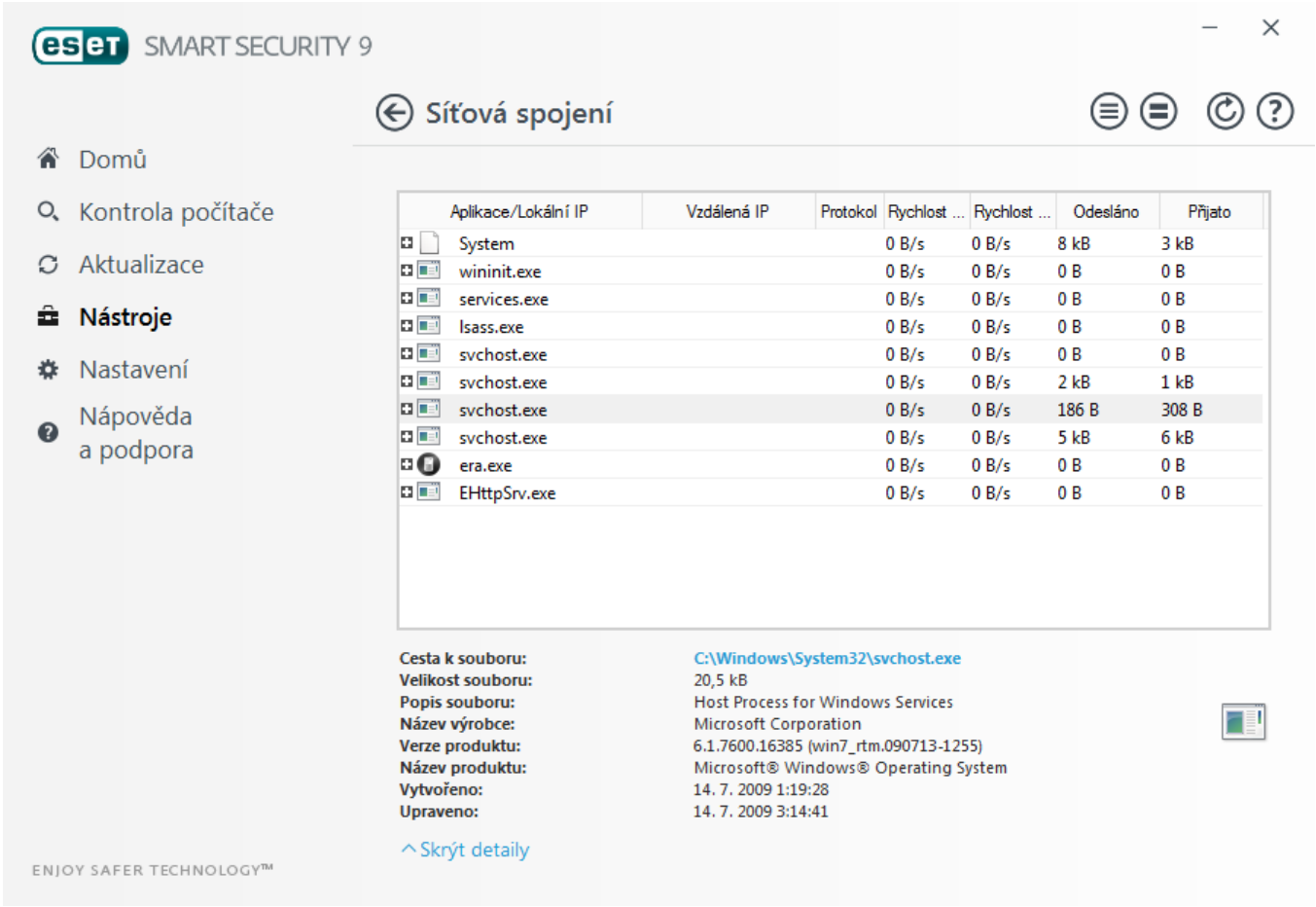
- **Krok: 1 sekunda** – graf se obnoví každou sekundu a časová osa zobrazuje posledních 10 minut,
- **Krok: 1 minuta (posledních 24 hodin)** – graf se obnoví každou minutu a časová osa zobrazuje posledních 24 hodin,
- **Krok: 1 hodina (poslední měsíc)** – graf se obnoví každou hodinu a zobrazuje poslední měsíc,
- **Krok: 1 hodina (vybraný měsíc...)** – graf se obnoví každou hodinu a zobrazuje vybraný měsíc. Pokud chcete zobrazit data z jiného měsíce, klikněte na tlačítko **Změnit měsíc**.

Vertikální osa grafu probíhající aktivity souborového systému reprezentuje množství přečtených dat (modrá) a zapsaných dat (červená). Obě tyto hodnoty jsou vyčísleny v KB/MB/GB. Pod grafem je zobrazena legenda, která zároveň slouží jako přepínač zobrazovaných hodnot. Po ponechání kurzoru na vybrané položce legendy se v grafu zobrazí pouze tato položka.

V rozbalovacím menu **Aktivita** je možné přepnout typ grafu na **Síťová aktivita**. Zobrazení je stejné jako při sledování aktivity souborového systému. Jediným rozdílem je, že se v grafu zobrazuje objem dat stažených dat (červeně) a odeslaných dat (modře) v síti.

4.6.1.5 Síťová spojení

V okně **Síťová spojení** je zobrazen seznam spojení, která jsou navázána, nebo čekají na navázání spojení. Tím získáte přehled o aplikacích, které komunikují se vzdálenou stranou.



V prvním řádku se nachází jméno aplikace, aktuální rychlost přenášených dat a celkové množství přenesených dat. Seznam připojení dané aplikace s podrobnými informacemi rozbalíte kliknutím na **+**.

Sloupce

Aplikace/Lokální IP – název aplikace, lokální IP adresy a porty, na kterých probíhá komunikace.

Vzdálená IP – IP adresa a port vzdáleného počítače.

Protokol – použitý transportní protokol.

Rychlost ven/Rychlost dovnitř – aktuální rychlost odchozích a příchozích dat.

Odesláno/Přijato – celkový objem přijatých a odeslaných dat.

Zobrazit detaily – zobrazí podrobné informace o spojeních.

Kliknutím na **Nastavení zobrazených spojení...** zobrazíte rozšířené nastavení Síťového spojení, kde jsou dostupné následující možnosti:

Překládat IP adresy na názvy počítačů – je-li to možné, síťové adresy se uvádějí ve formě názvu DNS, nikoli v číselné podobě IP adresy,

Zobrazovat pouze TCP spojení – mezi spojení jsou zahrnuta pouze ta, která patří k protokolu TCP,

Zobrazit naslouchající spojení – zobrazena jsou také spojení, ve kterých neprobíhá komunikace, ale port je v systému otevřený a čeká na spojení,

Zobrazit spojení v rámci počítače – zobrazí se také spojení, jejichž vzdáleným protějškem je lokální systém. Jedná se o spojení typu localhost.

Kliknutím pravým tlačítkem myší na dané spojení se zobrazíte následující možnosti:

Zablokovat komunikaci pro dané spojení – ukončí danou komunikaci. Tato možnost se zobrazí pouze po kliknutí na aktivní spojení,

Rychlost obnovení – slouží pro nastavení intervalu, ve kterém se budou automaticky obnovovat informace o aktivních síťových spojeních,

Obnovit nyní – znovu načte/obnoví okno Síťové spojení.

Následující dvě možnosti se zobrazí pouze po kliknutí na aplikaci nebo proces, nikoli na aktivní spojení:

Dočasně zablokovat komunikaci pro daný proces – aktuální spojení aplikace bude zakázáno. Při vytvoření nového spojení se použije nastavení ze standardního pravidla firewallu. Popis nastavení naleznete v kapitole Pravidla a zóny,

Dočasně povolit komunikaci pro daný proces – aktuální spojení aplikace bude povoleno. Při vytvoření nového spojení se použije nastavení ze standardního pravidla firewallu. Popis nastavení naleznete v kapitole Pravidla a zóny.

4.6.1.6 ESET SysInspector

ESET SysInspector je aplikace, která slouží k získání podrobných informací o systému zahrnující seznam nainstalovaných ovladačů a programů, síťových připojeních a důležitých údajů z registru. Tyto informace mohou být užitečné při zjišťování příčiny podezřelého chování systému ať už vlivem nekompatibility software/hardware nebo infekce škodlivého kódu.

V okně SysInspector se nachází informace o vytvořených protokolech:

- **Čas** – čas vytvoření,
- **Komentář** – stručný komentář k vytvořenému záznamu,
- **Uživatel** – jméno uživatele, který vytvořil záznam,
- **Stav** – stav vytvoření.

Dostupné jsou následující akce:

- **Otevřít** – zobrazí vytvořený záznam. Případně klikněte pravým tlačítkem na vybraný záznam a z kontextového menu vyberte možnost **Zobrazit**.
- **Porovnat** – porovná dva vytvořené záznamy,
- **Přidat** – vytvoří nový záznam. Vyčkejte na dokončení protokolu ESET SysInspector (po dokončení se ve sloupci *Stav* zobrazí **Vytvořeno**),
- **Odstranit** – odebere záznam ze seznamu.

Po kliknutí pravým tlačítkem myši na konkrétní záznam jsou kromě výše uvedených dostupné další možnosti:

- **Zobrazit** – otevře vybraný protokol v ESET SysInspector (stejné jako dvojklik na vybraný záznam),
- **Porovnat** – porovná dva vytvořené záznamy,
- **Vytvořit...** – vytvoří nový záznam. Vyčkejte na dokončení protokolu ESET SysInspector (po dokončení se ve sloupci *Stav* zobrazí **Vytvořeno**),
- **Odstranit** – odstraní vybraný záznam,
- **Odstranit vše** – vymaže všechny záznamy,
- **Exportovat...** – uloží záznamy do *.XML* souboru nebo do zazipovaného *.XML* souboru.

4.6.1.7 Plánovač

Plánovač spravuje a spouští naplánované úlohy s předem nakonfigurovaným nastavením.

Plánovač je dostupný v hlavním okně programu ESET Smart Security na záložce **Nástroje** > **Plánovač**. Plánovač obsahuje přehledný seznam všech naplánovaných úloh, jejich nastavení a vlastností, které se provádějí ve stanovený čas pomocí definovaných profilů.

Plánovač slouží k plánování úloh jako je např. aktualizace programu, kontrola disku, kontrola souborů spouštěných po startu nebo pravidelná údržba protokolů. Přímo z hlavního okna můžete **Přidat** nebo **Odstranit** úlohu kliknutím na příslušné tlačítko. Kontextové menu, které se otevře po kliknutí pravým tlačítkem myši v okně plánovače, umožňuje následující akce: zobrazení detailních informací o úloze, okamžité provedení úlohy, přidání nové úlohy, úpravu resp. odstranění již existující úlohy. Zaškrtávacím tlačítkem vedle úkolu je možné úlohu deaktivovat.

Standardně **Plánovač** zobrazuje následující naplánované úlohy:

- **Údržba protokolů,**
- **Pravidelná automatická aktualizace,**
- **Automatická aktualizace po modemovém spojení,**
- **Automatická aktualizace po přihlášení uživatele,**
- **Kontrola souborů spouštěných po startu** (při přihlášení uživatele na počítač),
- **Kontrola souborů spouštěných po startu** (při úspěšné aktualizaci virových databází),
- **Automatická prvotní kontrola.**

Nastavení existujících naplánovaných úloh (a to jak předdefinovaných, tak vlastních) můžete měnit přes kontextové menu kliknutím na možnost **Změnit...**, nebo vybráním požadované úlohy, kterou chcete změnit, a kliknutím na tlačítko **Změnit**.

Přidání nové úlohy

1. Klikněte na tlačítko **Přidat** ve spodní části okna.
2. Zadejte název úlohy.
3. Vyberte požadovaný typ úlohy:

- **Spuštění externí aplikace** – poskytne výběr aplikace, kterou má plánovač spustit,
- **Údržba protokolů** – defragmentace odstraní prázdné záznamy v protokolech. Viditelné zlepšení práce s protokoly po optimalizaci je především při větším množství záznamů v protokolech,
- **Kontrola souborů spouštěných při startu** – kontroluje soubory, které se spouštějí při startu nebo po přihlášení do systému,
- **Vytvoření záznamu o stavu počítače** – vytvoří záznam systému pomocí ESET SysInspector, který slouží k důkladné kontrole stavu počítače a umožňuje zobrazit získané údaje v jednoduché a čitelné formě,
- **Volitelná kontrola počítače** – provede volitelnou kontrolu disků, jednotlivých složek a souborů na počítači,
- **Prvotní kontrola** – standardně se spustí po 20 minutách od instalace produktu nebo restartování počítače,
- **Aktualizace** – zajišťuje aktualizaci virových databází i aktualizaci všech programových komponent systému.

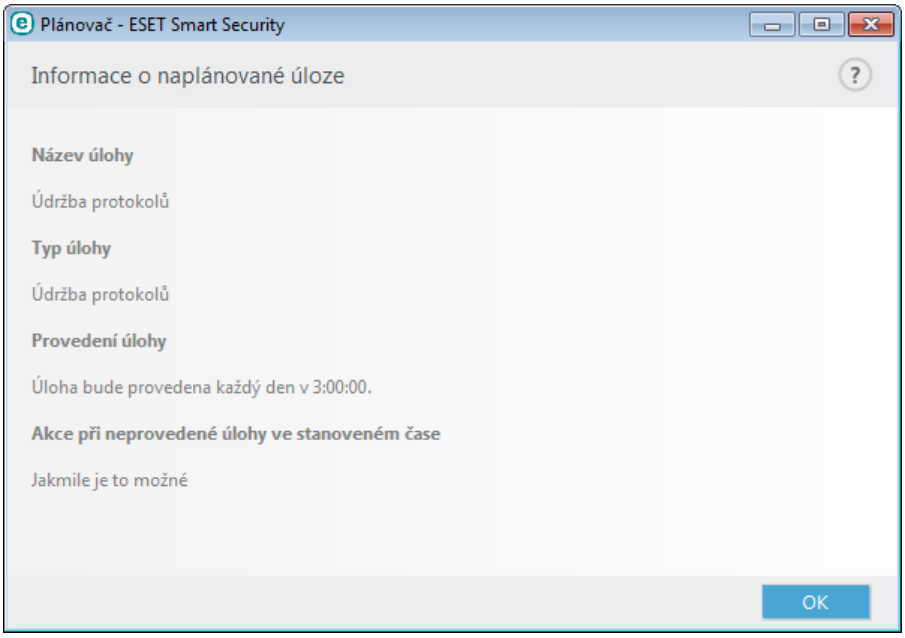
4. Pro aktivování úlohy přepněte přepínač do polohy **Zapnuto** (to můžete udělat kdykoli později přímo v seznamu naplánovaných úloh) a po kliknutí na tlačítko **Další** vyberte interval opakování:

- **Jednou** – úloha se provede pouze jednou v naplánovaném čase.
- **Opakovaně** – úloha se bude provádět opakovaně jednou za x hodin.
- **Denně** – úloha se provede každý den ve stanový čas.
- **Týdně** – úloha se bude provádět v určitý den/dny v týdnu ve stanoveném čase.
- **Při události** – úloha se provede při určité situaci.

5. Pokud chcete minimalizovat dopad na systémové zdroje při běhu notebooku na baterii nebo počítače z UPS, aktivujte možnost **Nespouštět úlohu, pokud je počítač napájen z baterie**. Po kliknutí na tlačítko Další zadejte **Čas provedení úlohy**. Pokud nebude možné úlohu v daném čase spustit, nastavte alternativní termín pro spuštění úlohy:

- **Při dalším naplánovaném termínu**
- **Jakmile to bude možné**
- **Okamžitě, pokud od posledního provedení uplynul stanovený interval** (definovaný v poli **Čas od posledního spuštění**)

Informace o naplánované úloze si můžete kdykoli zobrazit po kliknutí pravým tlačítkem myši na úlohu a vybrání možnosti **Zobrazit detaily úlohy**.



4.6.1.8 ESET SysRescue

ESET SysRescue je nástroj, který umožňuje vytvořit bootovatelný disk obsahující produkt ESET Security – tedy ESET NOD32 Antivirus, ESET Smart Security nebo jiný produkt určený pro servery. Hlavní výhodou ESET SysRescue je fakt, že ESET Security běží zcela nezávisle na aktuálně nainstalovaném operačním systému, přičemž má přímý přístup k disku a celému souborovému systému. Díky tomu je takto možné například odstranit infiltraci, kterou nebylo možné vymazat standardním způsobem při spuštěném operačním systému apod.

4.6.1.9 ESET LiveGrid®

ESET LiveGrid® (nová generace ESET ThreatSense.Net) je pokročilý systém varování před novými hrozbami pracující na základě reputace. Využívá aktuální informace z cloudu a umožňuje tak specialistům z virových laboratoří ESET udržovat ochranu před hrozbami na nejvyšší možné úrovni. Přímo z hlavní okna programu nebo kontextového menu můžete zkontrolovat reputaci běžících procesů a souborů a získat bližší informace z ESET LiveGrid®. Již při instalaci ESET Smart Security máte na výběr dvě možnosti:

1. Můžete vypnout ESET LiveGrid®. Neovlivní to žádnou součást programu a stále budete mít k dispozici nejlepší možnou ochranu,
2. Můžete ESET LiveGrid® nakonfigurovat pro odesílání anonymních informací o nových hrozbách. Takový soubor bude odeslán do virové laboratoře společnosti ESET k analyzování, což zajistí rychlejší vydání aktualizace virové databáze.

ESET LiveGrid® shromažďuje z vašeho počítače pouze informace, které se týkají nové infiltrace. To může zahrnovat vzorek nebo kopii souboru, ve kterém se infiltrace objevila, název složky, kde se soubor nacházel, název souboru, informaci o datu a čase detekce, způsob, jakým se infiltrace dostala do počítače a informaci o používaném operačním systému.

Standardně ESET Smart Security odesílá podezřelé soubory na podrobnou analýzu do virové laboratoře ESET. Pokud se infiltrace nachází v souborech s určitými příponami, jako například *.doc* a *.xls*, nikdy se neodesílá jejich obsah.

Mezi výjimky můžete přidat další přípony souborů, jejichž obsah nechcete odesílat.

Pro přístup k nastavení ESET LiveGrid® přejděte do **Rozšířeného nastavení** (po stisknutí klávesy F5 v hlavním okně programu) na záložku **Nástroje** > **ESET LiveGrid®**.

Zapnout ESET LiveGrid® (doporučeno) – systém ESET LiveGrid® pracující na základě reputace zvyšuje účinnost antivirového řešení ověřováním souborů vůči online databázi povolených a zakázaných souborů.

Odesílat anonymní statistiky – tato možnost je standardně zapnuta. Zrušením této možnosti zakážete odesílání anonymních dat o vašem počítači do ESET LiveGrid®. Tyto informace mohou obsahovat název infiltrace, datum a čas detekce, verzi ESET Smart Security, verzi používaného operačního systému a místní nastavení.

Odesílat soubory – tato možnost je standardně zapnuta. Podezřelé soubory, pravděpodobné infiltrace nebo nežádoucí chování bude odesíláno do společnosti ESET prostřednictvím technologie ESET LiveGrid®.

Po aktivování možnosti **Zapisovat do protokolu** se budou do protokolu zaznamenávat všechny informace o odeslaných datech. Při odeslání souboru nebo statistických dat se informace zobrazí v Protokolech.

Kontaktní e-mail (nepovinný údaj) – zadaný kontaktní e-mail se odešle společně s podezřelým souborem a v případě potřeby může být použit pro vyžádání dalších informací. Prosím, mějte na paměti, že od společnosti ESET neobdržíte žádnou informaci o zaslaném vzorku, pokud nejsou vyžadovány podrobnější informace k jeho analyzování.

Výjimky – pomocí seznamu výjimek můžete vyloučit složky a konkrétní typy souborů z odeslání k analýze (například soubory obsahující citlivé informace jako dokumenty nebo tabulky). Seznam zobrazených souborů a složek nebude nikdy odeslán do virových laboratoří ESET k další analýze na přítomnost škodlivého kódu. Standardně se neodesílají nejrozšířenější typy souborů (.doc atp.) a v případě potřeby můžete tento seznam kdykoli rozšířit.

Pokud jste měli zapnutý ESET LiveGrid® a nyní jste jej vypnuli, může se stát, že v počítači jsou již připraveny datové balíčky k odeslání. Tyto balíčky se ještě odešlou při nejbližší příležitosti. Po vypnutí systému se již nové balíčky vytvářet nebudou.

4.6.1.9.1 Podezřelé soubory

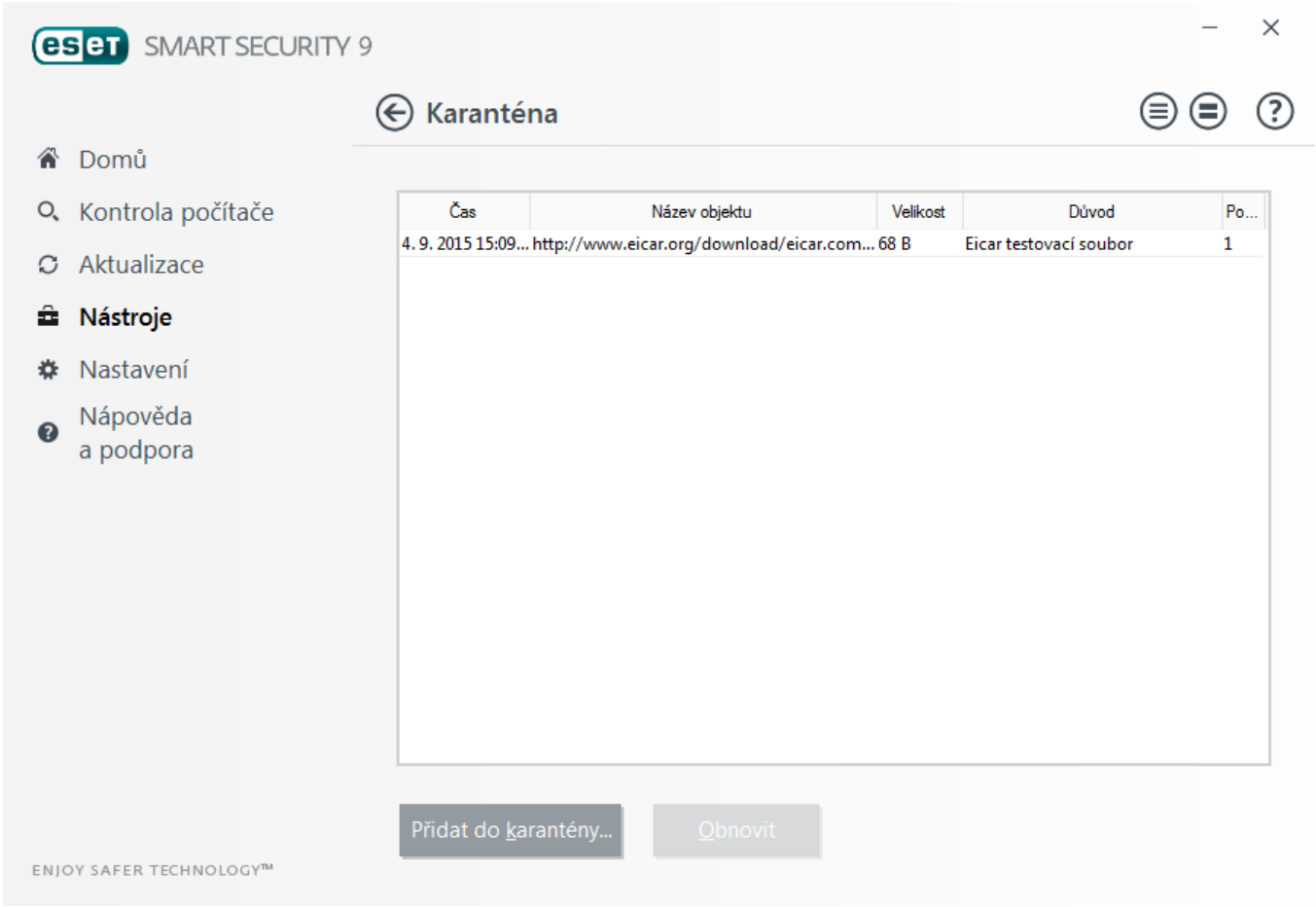
Po kliknutí na **Změnit** na řádku **Výjimky** na záložce ESET LiveGrid® můžete nastavit, jakým způsobem budou podezřelé soubory odesílány do virové laboratoře společnosti ESET.

Pokud naleznete podezřelý soubor, můžete jej odeslat k analýze do naší virové laboratoře. V případě, že jedná o nebezpečnou aplikaci, její detekce bude přidána v některé z nejbližších aktualizací virové databáze.

4.6.1.10 Karanténa

Hlavním úkolem karantény je bezpečné uchovávání infikovaných souborů. Ve většině případů se může jednat o soubory, které není možné vyléčit, není jisté, zda je bezpečné jejich odstranění, případně se jedná o chybnou detekci antivirové ochrany ESET Smart Security.

Do karantény můžete ručně přidat jakýkoli soubor. To je vhodné v případě, kdy podezřelý soubor nebyl detekován antivirovým skenerem. Soubory z karantény můžete zaslat k analýze do virové laboratoře společnosti ESET.



Soubory uložené v karanténě si můžete prohlédnout v přehledné tabulce včetně informací o datu a čase přidání souboru do karantény, cesty k původnímu umístění souboru, jeho velikosti v bajtech, důvodu proč byl přidán do karantény (např. objekt přidaný uživatelem) a počtu infiltrací (např. pokud archiv obsahoval více infikovaných souborů).

Přidání do karantény

ESET Smart Security přidává soubory do karantény automaticky při jejich vymazání (pokud jste tuto možnost v okně s upozorněním nezrušili). Pokud uznáte za vhodné, může pomocí tlačítka **Přidat do karantény...** do karantény přidat podezřelý soubor ručně. V takovém případě se však soubor ze svého původního umístění nesmaže. Kromě tlačítka **Přidat do karantény...** lze tuto akci provést kliknutím pravým tlačítkem myši v okně **Karantény** a vybrat možnost **Přidat do karantény...**.

Obnovení z karantény

Soubory uložené v karanténě můžete vrátit do jejich původního umístění, odkud byly vymazány. Slouží k tomu funkce **Obnovit**, která je rovněž přístupná také z kontextového menu po kliknutí pravým tlačítkem myši na daný soubor v karanténě. V kontextovém menu se dále nachází možnost **Obnovit do...**, která dokáže obnovit soubor na jiné místo, než to, ze kterého byl původně smazán. Pokud se jedná o potenciálně nechtěnou aplikace, v takovém případě bude v kontextovém menu dostupná možnost **Obnovit a vyloučit z kontroly**. Pro více informací o tomto typu aplikací přejděte do slovníku pojmů.

Odstranění z karantény – klikněte pravým tlačítkem na objekt v karanténě z kontextového menu vyberte možnost **Odstranit z karantény**. Případně vyberte objekt a stiskněte klávesu **Delete**.

Poznámka: Pokud program do karantény umístil soubor z důvodu falešného poplachu, vytvořte pro něj výjimku z kontroly a zašlete jej na technickou podporu společnosti ESET.

Odeslání souboru z karantény k analýze

Pokud máte v karanténě uložen soubor s podezřelým chováním, můžete jej odeslat do společnosti ESET k analýze. Vyberte daný soubor, klikněte na něj pravým tlačítkem myši a z kontextového menu vyberte možnost **Odeslat k analýze**.

4.6.1.11 Proxy server

Ve velkých lokálních sítích, může připojení do internetu zajišťovat tzv. proxy server. V takovém případě musí být proxy server správně zadán v nastavení programu, jinak by mohlo dojít k potížím se stahováním aktualizací. Nastavení proxy serveru je možné v ESET Smart Security definovat na dvou odlišných místech v rámci Rozšířeného nastavení.

V prvním případě můžete konfigurovat proxy server v části **Nástroje** > **Proxy server**. Definování proxy serveru na této úrovni má pro ESET Smart Security důsledek globálního nastavení proxy serveru. Nastavení budou používat všechny moduly vyžadující přístup k internetu.

Pro nastavení proxy serveru na této úrovni vyberte možnost **Používat proxy server** a následně zadejte adresu proxy serveru do pole **Proxy server** a číslo portu do pole **Port**.

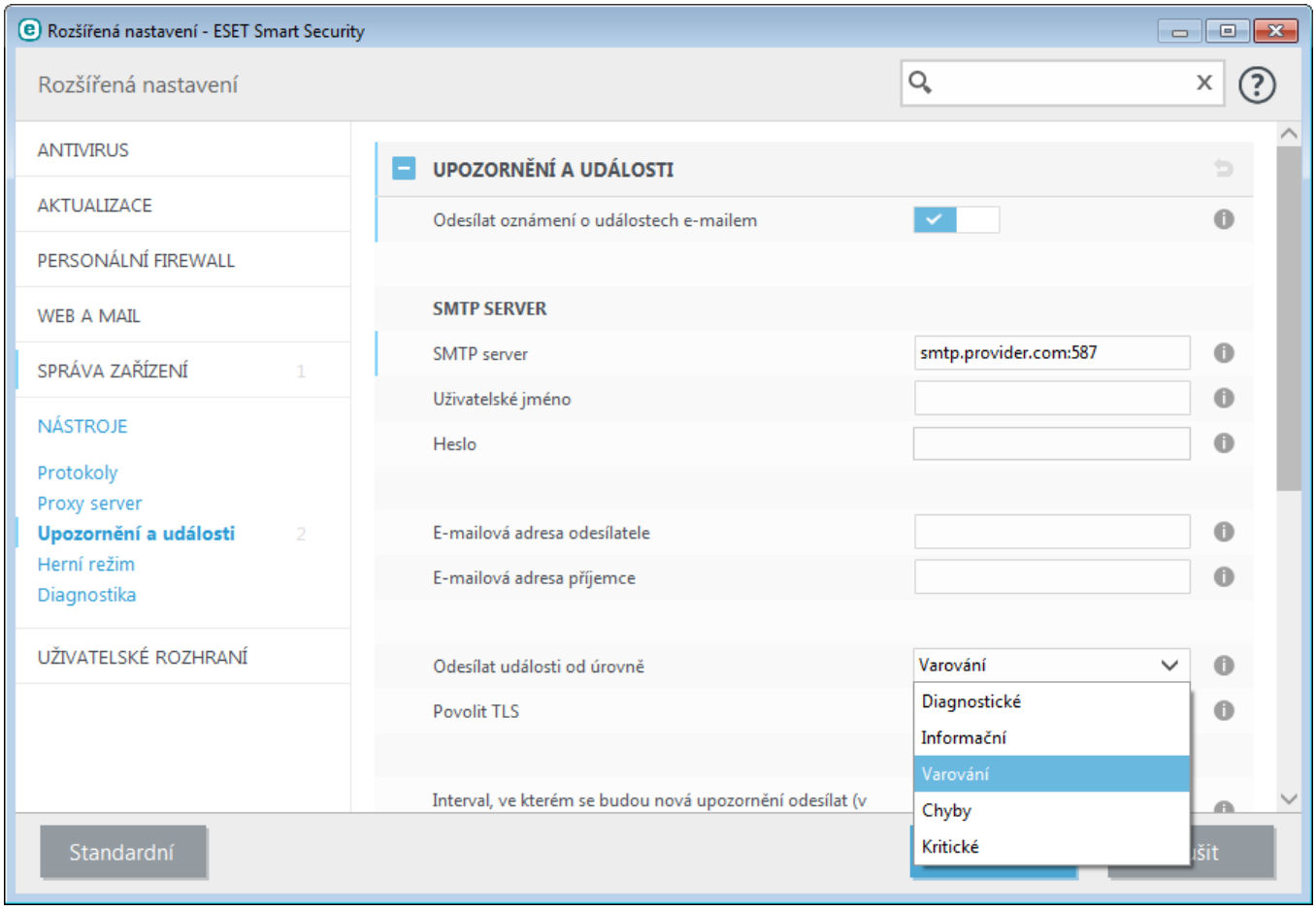
V případě, že komunikace s proxy serverem vyžaduje autentifikaci, je potřeba také zaškrtnout pole **Proxy server vyžaduje autorizaci** a zadat patřičné údaje do polí **Uživatelské jméno** a **Heslo**. Pro získání automatického nastavení proxy serveru můžete kliknout na tlačítko **Vyhledat proxy...**, tímto se přenese nastavení z programu Internet Explorer.

Poznámka: Tímto způsobem není možné získat autentifikační údaje (uživatelské jméno a heslo), které v případě potřeby musíte zadat ručně.

V druhém případě se nastavení proxy serveru nachází v **Rozšířeném nastavení** na záložce **Aktualizace**. Toto nastavení je platné pro konkrétní profil aktualizace a je vhodné jej použít, pokud se jedná o přenosný počítač, který provádí aktualizaci z různých míst. Bližší popis nastavení naleznete v kapitole Pokročilé nastavení aktualizace.

4.6.1.12 Upozornění a události

ESET Smart Security dokáže odesílat e-maily při výskytu události s nastavenou úrovní důležitosti. Pomocí možnosti **E-mailem odesílat oznámení o událostech** aktivujete tuto funkci a zasílání upozornění e-mailem.



Poznámka: ESET Smart Security podporuje SMTP servery využívající šifrování.

SMTP server

SMTP server – adresa SMTP serveru prostřednictvím kterého budou zprávy odesílány (například *smtp.provider.com:587*, pokud nespecifikujete port, použije se výchozí 25).

Uživatelské jméno a **Heslo** – v případě, že SMTP server vyžaduje autorizaci, musíte vyplnit tato pole pro přístup k SMTP.

E-mailová adresa odesílatele – specifikuje adresu odesílatele, která se použije v hlavičce e-mailové zprávy.

E-mailová adresa příjemce – specifikuje adresu příjemce, která se použije v hlavičce e-mailové zprávy.

Odesílat události od úrovně – specifikuje, od které úrovně důležitosti se budou upozornění na události odesílat.

- **Diagnostické** – e-mailem se odešlou diagnostické informace pro řešení problémů a všechny níže uvedené záznamy.
- **Informativní** – e-mailem se odešlou informace o nestandardních síťových událostech.
- **Varování** – e-mailem se odešlou upozornění na chyby a varovné zprávy (například Anti-stealth není funkční nebo selhala aktualizace virové databáze.
- **Chyby** – e-mailem se odešlou upozornění na chybové stavy aplikace (například nefunkční ochrana dokumentů).
- **Kritické** – e-mailem se odešlou upozornění na kritické stavy aplikace (například problém s antivirovou ochranou nebo upozornění na infiltraci v systému).

Povolit TLS – umožní odesílání zpráv prostřednictvím zabezpečeného TLS spojení.

Interval, ve kterém se budou nová upozornění odesílat (v min.) – interval v minutách, po jehož uplynutí bude odeslán souhrnný e-mail se všemi upozorněními na událostí, které se v daném intervalu vyskytly. Pokud nastavíte

hodnotu na 0, upozornění bude odesláno okamžitě po jeho výskytu.

Odesílat každé upozornění v samostatném e-mailu – pokud je tato možnost aktivní, příjemce obdrží při výskytu události nové upozornění. Při výskytu velkého množství událostí v krátkém čase obdrží příjemce velké množství e-mailů.

Formát zprávy

Formát události – formát zprávy, která se zobrazí na vzdáleném počítači.

Formát varovné zprávy – přednastavený formát zpráv je vhodný pro většinu situací. Měnit jej doporučujeme pouze v ojedinělých případech.

Použít znaky národní abecedy – převede e-mailovou zprávu do ANSI kódování, které je nastaveno v regionálním nastavení systému Windows (např. windows-1250). Pokud ponecháte tuto možnost nezaškrtnutou, zpráva se převede do ASCII 7-bit (v takovém případě se například znak "á" změní na "a" a neznámý symbol bude označen nahrazen otazníkem "?").

Použít kódování pro znaky národní abecedy – e-mailová zpráva bude zakódována do Quoted-printable (QP) formátu, který využívá ASCII znaky, čímž se mohou bezchybně přenášet prostřednictvím e-mailu speciální (národní) znaky v 8-bitovém formátu (áéíóú).

4.6.1.12.1 Formát zprávy

Můžete definovat formát zpráv, které se odesílají na vzdálené počítače při výskytu dané události.

Upozornění na hrozby a informační oznámení mají přednastavený formát. Měnit jej doporučujeme pouze v ojedinělých případech, například pokud používáte automaticky systém pro zpracovávání e-mailů.

Ve formátu zpráv se nacházejí klíčová slova označená procentem (%), která jsou při vytváření zpráv nahrazena odpovídajícími hodnotami. Dostupná jsou následující klíčová slova:

- **%TimeStamp%** – datum a čas události,
- **%Scanner%** – modul, který zaznamenal událost,
- **%ComputerName%** – název počítače, na kterém došlo k události,
- **%ProgramName%** – program, který způsobil událost,
- **%InfectedObject%** – název škodlivého souboru, e-mailové zprávy apod.,
- **%VirusName%** – název infekce,
- **%ErrorDescription%** – popis chyby.

Klíčová slova **%InfectedObject%** a **%VirusName%** se používají pouze v upozorněních na hrozbu. Klíčové slovo **%ErrorDescription%** se používá pouze v informačních upozorněních.

Použít znaky národní abecedy – převede e-mailovou zprávu do ANSI kódování, které je nastaveno v regionálním nastavení systému Windows (např. windows-1250). Pokud ponecháte tuto možnost nezaškrtnutou, zpráva se převede do ASCII 7-bit (v takovém případě se například znak "á" změní na "a" a neznámý symbol bude označen jako "?").

Použít kódování pro znaky národní abecedy – e-mailová zpráva bude zakódována do Quoted-printable (QP) formátu, který využívá ASCII znaky, čímž se mohou bezchybně přenášet prostřednictvím e-mailu speciální (národní) znaky v 8-bitovém formátu (áéíóú).

4.6.1.13 Odesílání souborů analýze

Existuje možnost zaslání podezřelého souboru k analýze do společnosti ESET. Formulář k této akci naleznete na záložce **Nástroje** > **Odeslat soubor k analýze**. V případě, že máte soubor s podezřelým chováním nebo jste narazili na infikovanou stránku, můžete tato data odeslat na analýzu do virové laboratoře ESET. Pokud se ukáže, že se jedná o nebezpečnou aplikaci nebo webovou stránku, její detekce bude přidána v některé z nejbližších aktualizací.

Případně můžete soubory odesílat e-mailem. Pokud dáváte přednost této možnosti, prosím dbejte na to, abyste soubor přidali do archivu WinRAR/ZIP a ochránili archiv heslem "infected" předtím, než jej odešlete na adresu samples@eset.com. Prosím, uveďte také co nejvíce informací o zahrnující výrobce, verzi produktu a také internetové adrese, ze které jste aplikaci (resp. soubor) stáhli.

Poznámka: Před odesláním souboru do společnosti ESET se ujistěte, že splňuje jedno z následujících kritérií:
- soubor není programem ESET detekován,
- soubor je detekován nesprávně jako hrozba.

Kontaktovat zpět vás budeme pouze v případě, že budeme potřebovat více informací.

Z rozbalovacího menu **Důvod odeslání souboru** vyberte možnost, která nejlépe vystihuje danou situaci:

- **Podezřelý soubor**
- **Podezřelá stránka** (webová stránka infikovaná malware)
- **Falešně detekovaný soubor** (soubor detekovaný jako infikovaný není infikovaný)
- **Falešně detekovaná stránka**
- **Ostatní**

Soubor/Stránka – cesta k souboru nebo URL adresa.

Kontaktní e-mail – na tento e-mail vás budou pracovníci virové laboratoře ESET kontaktovat, pokud budou potřebovat více informací. Zadání e-mailu je nepovinné. Na kontaktní e-mail nebude zaslána žádná odezva, protože denně do společnosti ESET chodí několik desítek tisíc souborů a není možné na každý e-mail reagovat.

4.6.1.14 Aktualizace operačního systému Windows

Aktualizace operačního systému Windows představují důležitou součást pro zajištění ochrany uživatelů před zneužitím bezpečnostních děr a tím pádem možným infikováním systému. Z tohoto důvodu je vhodné instalovat aktualizace Microsoft Windows co nejdříve po jejich vydání. V ESET Smart Security můžete nastavit, od jaké úrovně chcete být informováni na chybějících systémové aktualizace. Na výběr jsou následující možnosti:

- **Žádné aktualizace** – nebudou nabízeny žádné aktualizace,
- **Volitelné aktualizace** – budou nabízeny aktualizace s nízkou prioritou a všechny následující,
- **Doporučené aktualizace** – budou nabízeny běžné aktualizace a všechny následující,
- **Důležité aktualizace** – budou nabízeny důležité aktualizace a všechny následující,
- **Kritické aktualizace** – budou nabízeny pouze kritické aktualizace.

Kliknutím na tlačítko **OK** uložíte změny. Zobrazení okna dostupných aktualizací proběhne po ověření stavu na aktualizačním serveru. Samotné zobrazení dostupných aktualizací proto nemusí nutně proběhnout ihned po uložení změn.

4.7 Uživatelské rozhraní

V sekci **Uživatelské rozhraní** můžete konfigurovat nastavení uživatelského rozhraní (GUI).

V části prvky uživatelského rozhraní upravíte vzhled rozhraní a množství použitých efektů.

Pro zajištění maximální bezpečnosti a zabránění nežádoucím změnám v nastavení programu použijte sekci Přístup k nastavení.

Nastavením v sekci Upozornění a události změníte chování varování při detekci infekce a chování systémových upozornění. Tato oznámení si můžete nastavit dle svých potřeb.

Pokud se rozhodnete nezobrazovat určitá varování, jejich seznam naleznete v části **Stavy aplikací**. Zde můžete zjistit

jejich stav a případně znovu povolit jejich zobrazování.

Kontextové menu se zobrazí po kliknutí pravým tlačítkem myši na vybraný objekt. Tento nástroj použijte pro integraci ovládacích prvků ESET Smart Security do kontextového menu.

4.7.1 Prvky uživatelského rozhraní

ESET Smart Security umožňuje přizpůsobit nastavení pracovního prostředí programu vašim potřebám. Tyto možnosti jsou dostupné v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu) na záložce **Uživatelské rozhraní** > **Prvky uživatelského rozhraní**.

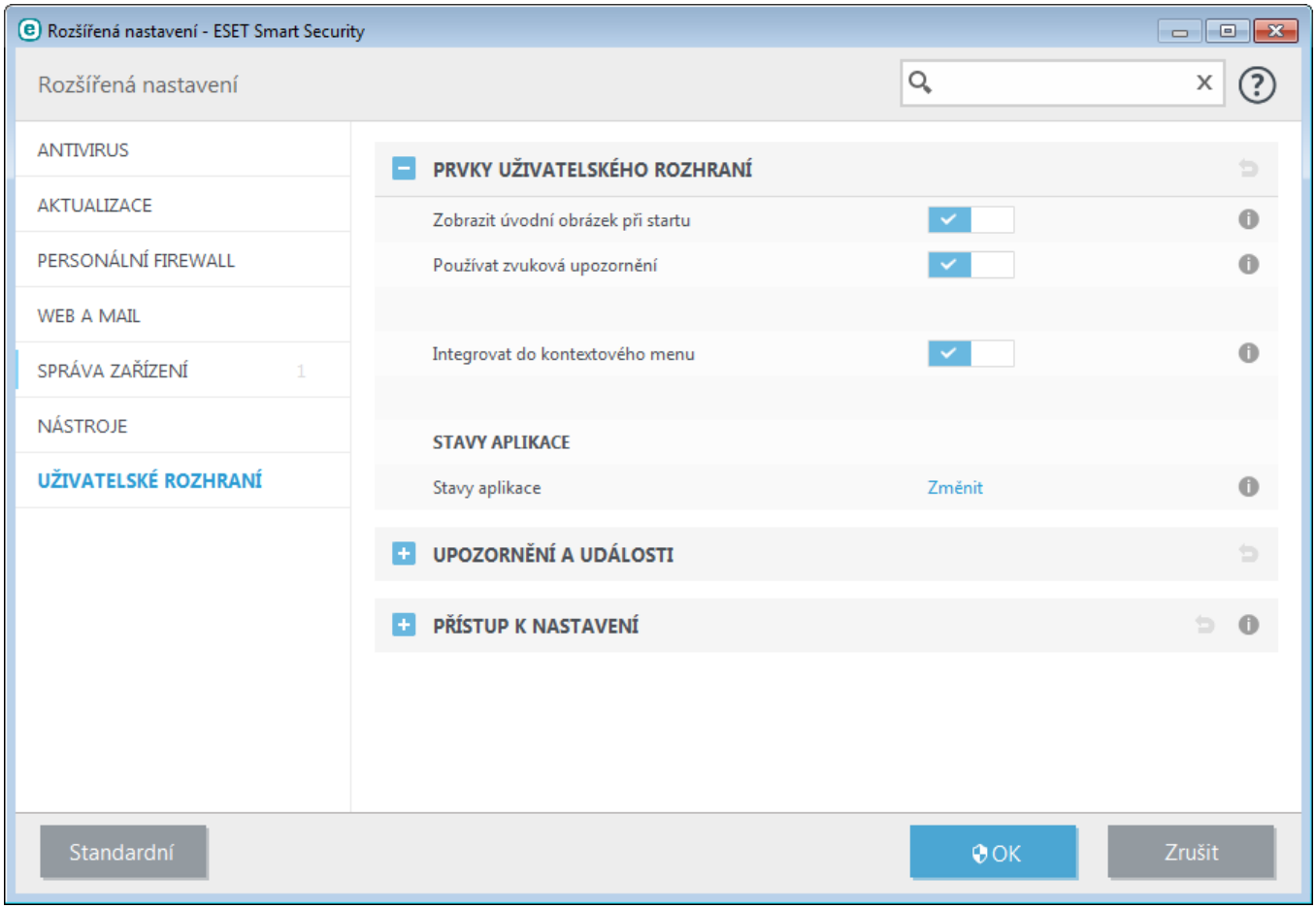
Pomocí možnosti **Zobrazit úvodní obrázek při startu** můžete zapnout nebo vypnout zobrazování úvodního obrázku při spouštění ESET Smart Security.

Pokud chcete, aby ESET Smart Security přehrával zvuky při důležitých událostech, zaškrtněte možnost **Používat zvuková upozornění**.

Integrovat do kontextového menu – integruje ovládací prvky ESET Smart Security do kontextového menu.

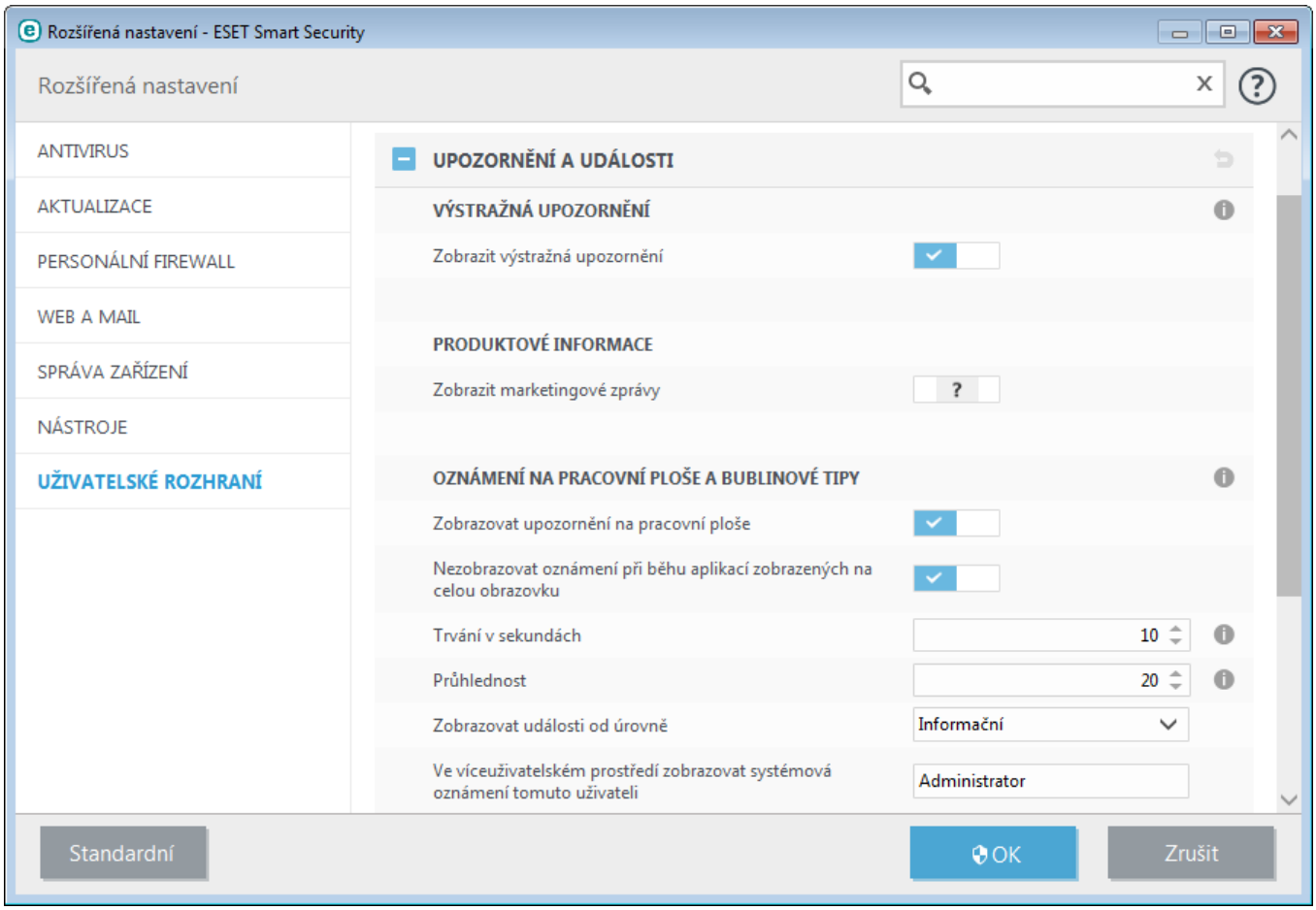
Stavy aplikace

Stavy aplikace – po kliknutí na **Změnit** můžete zapnout nebo vypnout zobrazování stavů aplikace v hlavním okně na záložce **Domů**.



4.7.2 Upozornění a události

Okno **Upozornění a události** se nachází v sekci **Uživatelské rozhraní** a umožňuje konfiguraci výstražných a informačních hlášení ESET Smart Security, například informace o úspěšné aktualizaci. Nastavit můžete dobu zobrazení a průhlednost bubliny s upozorněním (pouze na systémech, které to podporují).



Výstražná upozornění

Zobrazování všech oken s upozorněním vypnete odškrtnutím možnosti **Zobrazit výstražná upozornění**. Toto doporučujeme nastavit pouze ve specifických situacích. Pro většinu uživatelů doporučujeme ponechat tuto možnost aktivní.

Produktové informace

Zobrazit marketingové zprávy – prostřednictvím tohoto kanálu budeme uživatele informovat o novinkách a ESET akcích. Vypnutím této možnosti nebudete dostávat žádné marketingové informace.

Oznámení na pracovní ploše

Upozornění na ploše a bublinové tipy slouží pouze pro zobrazování informací a nenabízejí ani nevyžadují interakci uživatele. Zobrazují se v pravém dolním rohu obrazovky. Pro aktivování této možnosti zaškrtněte **Zobrazovat upozornění na pracovní ploše**. Pro další možnosti konfigurace jako je doba zobrazení upozornění a průhlednost tohoto okna upravíte pomocí možností zobrazených níže. Pokud nechcete zobrazovat oznámení nevyžadující interakci při běhu aplikací přes celou obrazovku, vyberte možnost **Nezobrazovat oznámení při běhu aplikací zobrazených na celou obrazovku**.

V rozbalovacím menu **Zobrazovat události od úrovně** můžete nastavit bezpečnostní úroveň, od které chcete být informováni.

- **Diagnostické** – obsahují informace důležité pro ladění programu a všechny níže uvedené záznamy,
- **Informační** – obsahují informační zprávy, například o úspěšné aktualizaci a všechny níže uvedené záznamy,
- **Varování** – obsahují varovné zprávy a kritické chyby,
- **Chyby** – obsahují chyby typu "Chyba při stahování souboru aktualizace" a kritické chyby,
- **Kritické chyby** – obsahují pouze kritické chyby (chyba při startu antivirové ochrany, atd...).

Poslední možností v tomto okně je nastavení příjemce zpráv ve víceuživatelských systémech. Do pole **Ve víceuživatelském prostředí posílat systémová hlášení tomuto uživateli** zadejte jméno uživatele, kterému bude ESET Smart Security zobrazovat systémová oznámení. Standardně by tímto uživatelem měl být administrátor systému nebo sítě. Tato možnost je vhodná pro terminálové systémy, kdy všechna systémová oznámení budou chodit jen administrátorovi.

Informační okna

Dobu zobrazení informačních upozornění nastavíte pomocí možnosti **Zavírat informační okna automaticky)**. Po uplynutí nastaveného času se okno s upozorněním zavře, pokud jej dříve nezavřete ručně.

Potvrzovací zprávy – pomocí této možnosti můžete ovlivnit, která dialogové se budou nebo nebudou zobrazovat.

4.7.2.1 Rozšířená nastavení

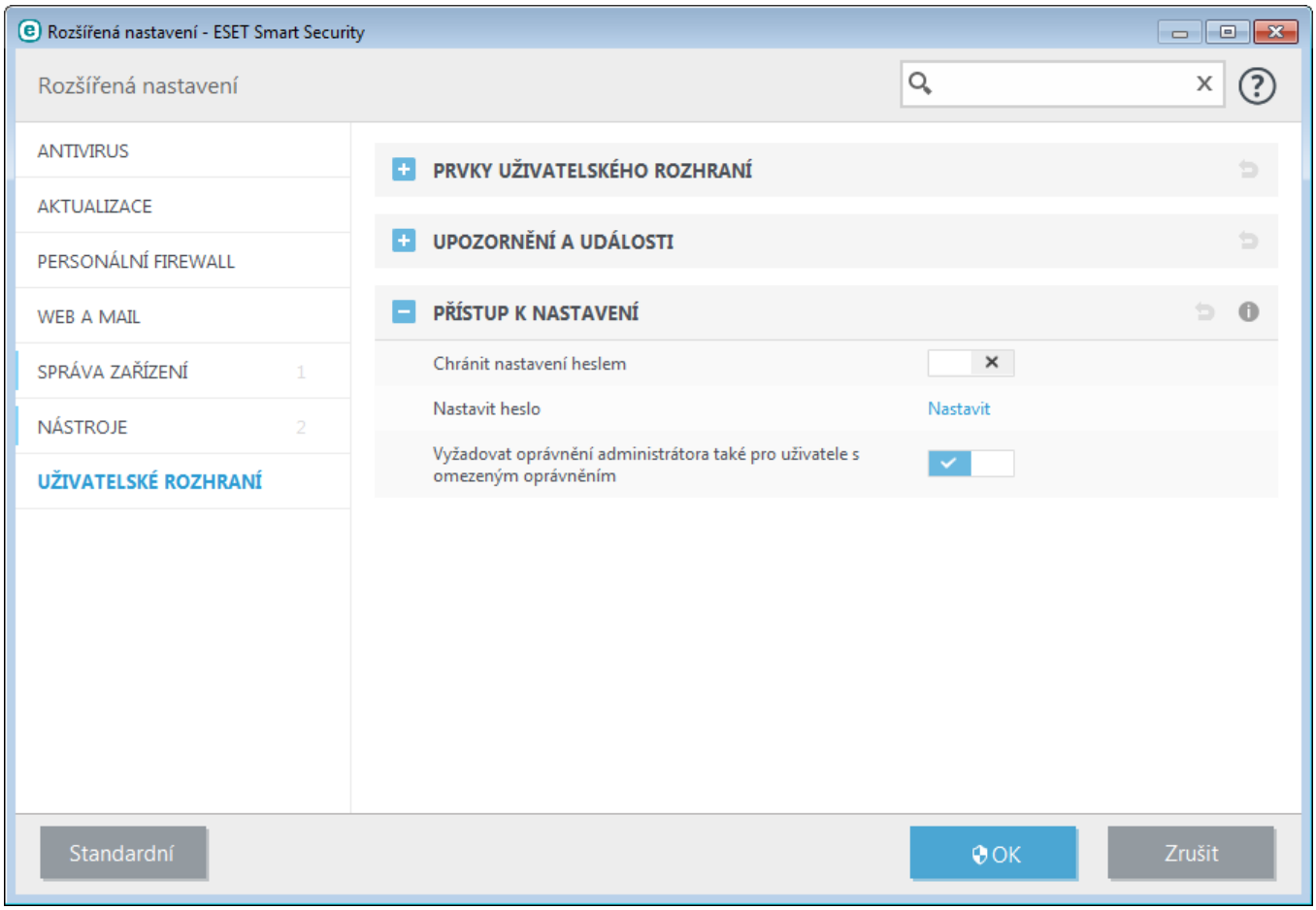
V rozbalovacím menu **Zobrazovat události od úrovně** můžete nastavit bezpečnostní úroveň, od které chcete být informováni.

- **Diagnostické** – obsahují informace důležité pro ladění programu a všechny níže uvedené záznamy,
- **Informační** – obsahují informační zprávy, například o úspěšné aktualizaci a všechny níže uvedené záznamy,
- **Varování** – obsahují varovné zprávy a kritické chyby,
- **Chyby** – obsahují chyby typu "Chyba při stahování souboru aktualizace" a kritické chyby,
- **Kritické chyby** – obsahují pouze kritické chyby (chyba při startu antivirové ochrany, Personálního firewallu, atd...).

Poslední možností v tomto okně je nastavení příjemce zpráv ve víceuživatelských systémech. Do pole **Ve víceuživatelském prostředí posílat systémová hlášení uživateli** zadejte jméno uživatele, kterému bude ESET Smart Security zobrazovat systémová oznámení. Standardně by tímto uživatelem měl být administrátor systému nebo sítě. Tato možnost je vhodná pro terminálové systémy, kdy všechna systémová oznámení budou chodit jen administrátorovi.

4.7.3 Přístup k nastavení

Správné nastavení ESET Smart Security je velmi důležité pro zachování celkové bezpečnosti systému a jeho neoprávněná změna může vést ke snížení stability a ochrany systému. Pro ochranu nastavení heslem přejděte v **Rozšířeném nastavení** (dostupném po stisknutí **klávesy F5** v hlavním okně programu) na záložku **Uživatelské rozhraní** > **Přístup k nastavení**).



Chránit nastavení heslem – zamkne/odemkne nastavení programu. Po kliknutí se zobrazí dialogové okno pro zadání hesla.

Pro nastavení změnu stávajícího hesla klikněte na **Nastavit heslo**.

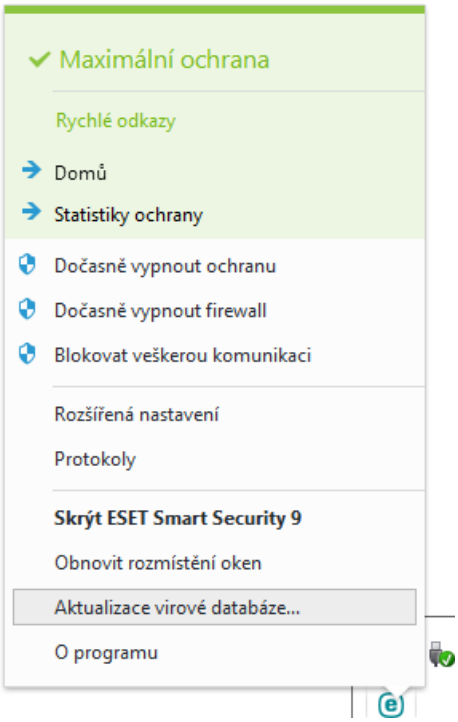
Vyžadovat oprávnění administrátora také pro uživatele s omezeným oprávněním – pokud přihlášený uživatel nemá administrátorská práva, pak při pokusu o změnu některých nastavení bude vyžadováno přihlášení administrátora (podobně jako je tomu ve Windows Vista a vyšších při zapnutém UAC). Taková změna zahrnuje vypnutí modulů ochrany nebo Personálního firewallu.

Dostupné pouze ve Windows XP:

Vyžadovat oprávnění administrátora (systém bez UAC) – po aktivování této možnosti bude ESET Smart Security vyžadovat zadání administrátorských přihlašovacích údajů.

4.7.4 Ikona v oznamovací oblasti

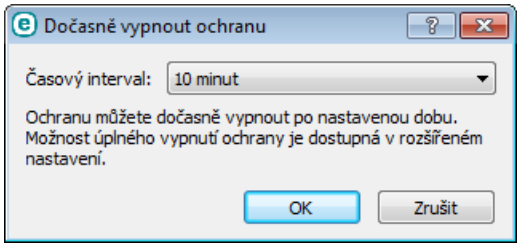
Nejdůležitější možnosti a funkce programu jsou dostupné přímo ze systémové oznamovací oblasti (v pravém dolním rohu obrazovky). Stačí kliknout pravým tlačítkem myši na ikonu programu .



Blokovat veškerou komunikaci – Personální firewall zablokuje veškerou odchozí a příchozí komunikaci v rámci sítě a internetu.

Dočasně vypnout ochranu – zobrazí potvrzovací dialog, pomocí kterého vypnete Antivirovou a antispywarovou ochranu – ta chrání systém proti škodlivým útokům tím, že kontroluje soubory, e-maily a komunikaci prostřednictvím internetu.

V rozbalovacím menu **Časový interval** můžete nastavit dobu, po kterou budou všechny součásti ochrany vypnuty.



Dočasně vypnout firewall – přepne firewall do neaktivního režimu. Pro více informací přejděte do kapitoly Síť.

Blokovat veškerou komunikaci – zablokuje veškerou síťovou komunikaci. Pro obnovení komunikace klikněte na **Povolit veškerou komunikaci**.

Rozšířená nastavení – po kliknutí se zobrazí Rozšířené nastavení programu. Jiný způsob, jak otevřít toto okno je stisknout klávesu **F5** v hlavním okně programu nebo kliknout na **Nastavení** > **Rozšířené nastavení**.

Protokoly – protokoly obsahují informace o všech systémových událostech a poskytují přehled o nalezených hrozbách.

Skrýt ESET Smart Security – skryje všechna otevřená okna ESET Smart Security.

Obnovit rozmístění oken – obnoví přednastavenou velikost a pozici okna ESET Smart Security na obrazovce.

Aktualizace virové databáze – spustí se aktualizace virové databáze pro zajištění maximální ochrany před škodlivým kódem.

O programu – poskytuje informace o systému, instalovaném programu ESET Smart Security a všech jeho

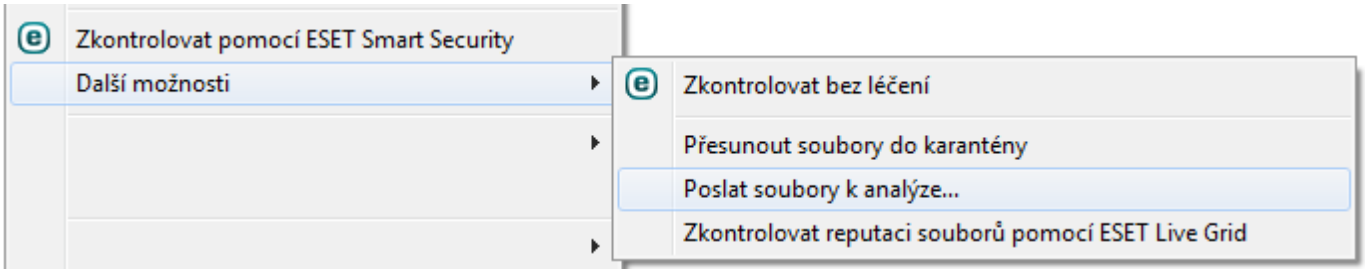
programovaných modulech. Také zde naleznete datum platnosti licence. Ve spodní části okna se nachází informace o operačním systému a systémových prostředcích.

4.7.5 Kontextové menu

Kontextové menu se zobrazuje po kliknutí pravým tlačítkem myši na daný objekt. V tomto menu jsou následně dostupné akce, které je možné na daném objektu provést.

Do kontextového menu můžete integrovat také ovládací prvky produktu ESET Smart Security. Podrobné nastavení této funkce je dostupné v Rozšířeném nastavení (po stisknutí klávesy F5 v hlavním okně programu) na záložce **Uživatelské rozhraní** > **Kontextové menu**.

Integrovat do kontextového menu – integruje ovládací prvky ESET Smart Security do kontextového menu.



5. Pokročilý uživatel

5.1 Správa profilů

Správa profilů se v programu ESET Smart Security používá na dvou místech – při **Volitelné kontrole počítače** a **Aktualizaci**.

Volitelná kontrola počítače

Oblíbená nastavení kontroly počítače si můžete uložit do profilů pro jejich opakované použití v budoucnu. Doporučujeme vytvořit několik profilů s různými cíli a metodami kontroly, případně s dalšími parametry.

Pro vytvoření nového profilu otevřete **Rozšířené nastavení** (dostupné po stisknutí klávesy F5 v hlavním okně programu), přejděte na záložku **Antivir** > **Volitelná kontrola počítače**. Kliknutím na **Změnit** na řádku **Profily** se zobrazí seznam existujících profilů kontroly počítače s možností vytvořit nový profil. V kapitole parametry skenovacího jádra ThreatSense naleznete popis jednotlivých parametrů pro nastavení kontroly počítače.

Příklad: Chcete vytvořit vlastní profil kontroly počítače a částečně vám vyhovuje nastavení předdefinovaného profilu **Smart kontrola počítače**, ale nechcete zároveň kontrolovat runtime archivy, potenciální nebezpečné aplikace a přitom požadujete **Přísné léčení**? Vytvořte nový profil kliknutím na tlačítko **Přidat** v Seznamu profilů Následně nově vytvořený profil vyberte z rozbalovacího menu **Aktivní profil** nastavte si parametry kontroly podle potřeby.

Aktualizace

Editor profilů umožňuje vytvořit nové aktualizační profily odlišné od standardního **Můj profil**. Ty se používají pouze v případě, že používáte různé způsoby připojení na aktualizační servery.

Příkladem může být firemní notebook, který se v interní síti aktualizuje z mirroru, ale mimo firemní síť se aktualizace stahují ze serverů společnosti ESET. Pro zajištění funkční aktualizace virové databáze vytvoříte dva profily, jeden pro firemní síť a druhý pro aktualizaci mimo firemní síť. Po vytvoření profilů je ještě potřeba odpovídajícím způsobem upravit naplánované úlohy na záložce **Nástroje** > **Plánovač**. Jeden profil bude primární, druhý jako sekundární.

Aktivní profil – aktuálně používaný profil. Pro jeho změnu vyberte jiný z rozbalovacího menu.

Seznam profilů – správa existujících aktualizačních profilů.

5.2 Klávesové zkratky

Pro rychlejší navigaci v produktu ESET můžete použít také následující klávesové zkratky:

F1	otevře nápovědu
F5	otevře Rozšířená nastavení
Šipka Nahoru/Dolů	pohyb mezi jednotlivými položkami
-	sbalí vybranou část strom pokročilého nastavení
TAB	přesune se na další položku v rámci okna
Esc	zavře aktivní dialogové okno

5.3 Diagnostika

Diagnostika poskytuje výpisy ze selhání běhu procesů programu ESET (například *ekrn.exe*). Pokud aplikace selže, vygeneruje se výpis, tzv. dump. Ten může pomoci vývojářům při ladění a opravě různých problémů v ESET Smart Security. Dostupné jsou dva typy výpisů:

- Vyberte možnost **Žádný** pro vypnutí této funkce.
- **Minimální** – zaznamená nejmenší sadu užitečných informací, které mohou pomoci identifikovat důvod, proč se aplikace nečekaně zastavila. Tento typ výpisu může být užitečný, pokud jste omezeni volným místem na disku. Nicméně, kvůli omezenému množství zahrnutých informací, chyby, které nebyly způsobeny přímo vláknem (thread) běžícím v době problému, nemusí být objeveny analýzou tohoto souboru.
- **Úplný** – zaznamená celý obsah systémové paměti, když se aplikace nečekaně zastaví. Kompletní výpis z paměti může obsahovat data procesů, které běžely v době, kdy byl výpis vytvořen.

Aktivovat diagnostické protokolování firewallu – Do souboru v PCAP formátu bude zaznamenána veškerá síťová komunikace vyhodnocována Personálním firewallem. Toto pomůže vývojářům při diagnostice a řešení problémů s modulem personálního firewallu.

Aktivovat diagnostické protokolování filtrování protokolů – do souboru v PCAP formátu bude zaznamenána veškerá síťová komunikace vyhodnocována Personálním firewallem. Toto pomůže vývojářům při diagnostice a řešení problémů s modulem filtrování protokolů.

Vytvořené protokoly naleznete ve složce:
C:\ProgramData\ESET\ESET Smart Security\Diagnostics ve Windows Vista a novějších nebo *C:\Documents and Settings\All Users\...* ve starších verzích operačního systému Windows.

Cílová složka – místo, kam se vygeneruje výpis při pádu.

Kliknutím na **Otevřít** zobrazíte obsah výše uvedené složky v novém okně *Průzkumníku Windows*.

5.4 Import a export nastavení

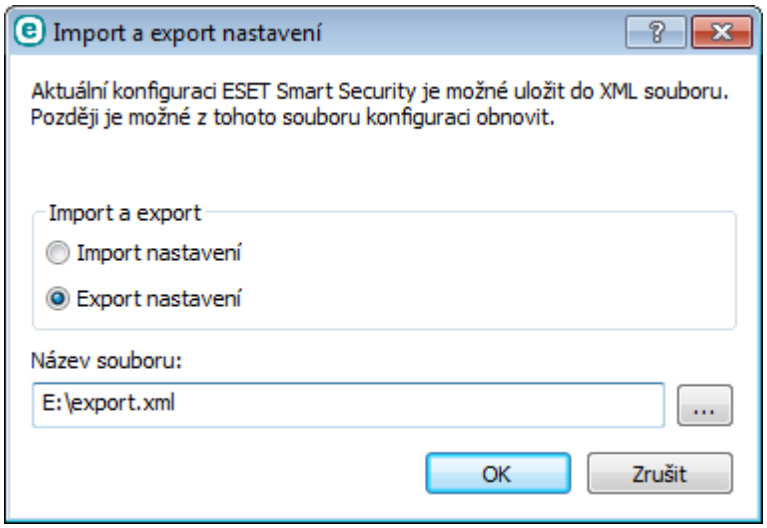
Na záložce **Nastavení** můžete do programu ESET Smart Security importovat nebo z něj naopak exportovat konfiguraci v .xml souboru.

Importování a exportování nastavení je užitečné například pokud si potřebujete zálohovat současné nastavení ESET Smart Security a chcete se k němu později vrátit. Export nastavení oceníte také v případě, že chcete stejné nastavení použít na více počítačích, kdy stačí pouze naimportovat daný .xml soubor.

Import nastavení je velmi jednoduchý. V hlavním okně programu klikněte na záložku **Nastavení** > **Import a export nastavení...**, vyberte možnost **Import nastavení** a kliknutím na tlačítko **...** najděte konfigurační soubor, který chcete importovat.

Export nastavení je velmi podobný importování. V případě, že potřebujete uložit aktuální nastavení ESET Smart Security, na záložce **Nastavení** klikněte na odkaz **Import a export nastavení**. Vyberte možnost **Export nastavení**, zadejte **Název souboru** (např. export.xml) a následně vyberte, kam chcete soubor s nastavením uložit.

Poznámka: Pokud nemáte přístup pro zápis do zadané složky, může dojít k chybě při exportování nastavení.



5.5 Detekce stavu nečinnosti

Možnosti detekce stavu nečinnosti počítače (idle) můžete konfigurovat v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu) na záložce **Antivirus** > **Kontrola při nečinnosti**. dokáže detekovat tyto stavy:

- aktivní spořič obrazovky,
- uzamčení počítače,
- odhlášení uživatele.

Pomocí přepínačů definujte stav, při kterém chcete provádět kontrolu počítače.

5.6 ESET SysInspector

5.6.1 Úvod do programu ESET SysInspector

ESET SysInspector je aplikace, která důkladně prohlédne počítač a zobrazí získaná data v souhrnném náhledu. Informace jako nainstalované ovladače a aplikace, síťová připojení nebo důležité položky registru Windows mohou pomoci při zjišťování příčiny podezřelého chování systému, ať už kvůli softwarové nebo hardwarové nekompatibilitě či infiltraci škodlivým kódme.

ESET SysInspector můžete spustit dvěma způsoby: Spuštěním přímo z řešení ESET Security nebo stažením samostatné verze (SysInspector.exe) z webových stránek společnosti ESET. Obě verze nabízejí identické funkce a ovládají se stejně. Rozdíl je pouze při zpracovávání výstupů. Samostatná verze exportuje záznam o systému do *.xml* souboru a uloží jej na pevný disk. Zatímco integrovaná verze uloží záznam o systému přímo do záložky **Nástroje** > **ESET SysInspector** (kromě ESET Remote Administrator). Pro více informací se podívejte do sekce ESET SysInspector jako součást ESET Smart Security.

Po spuštění ESET SysInspector chvíli vyčkejte na dokončení inspekce počítače. Může to trvat 10 sekund až několik minut v závislosti na hardwarové konfiguraci, operačním systému a počtu nainstalovaných aplikací.

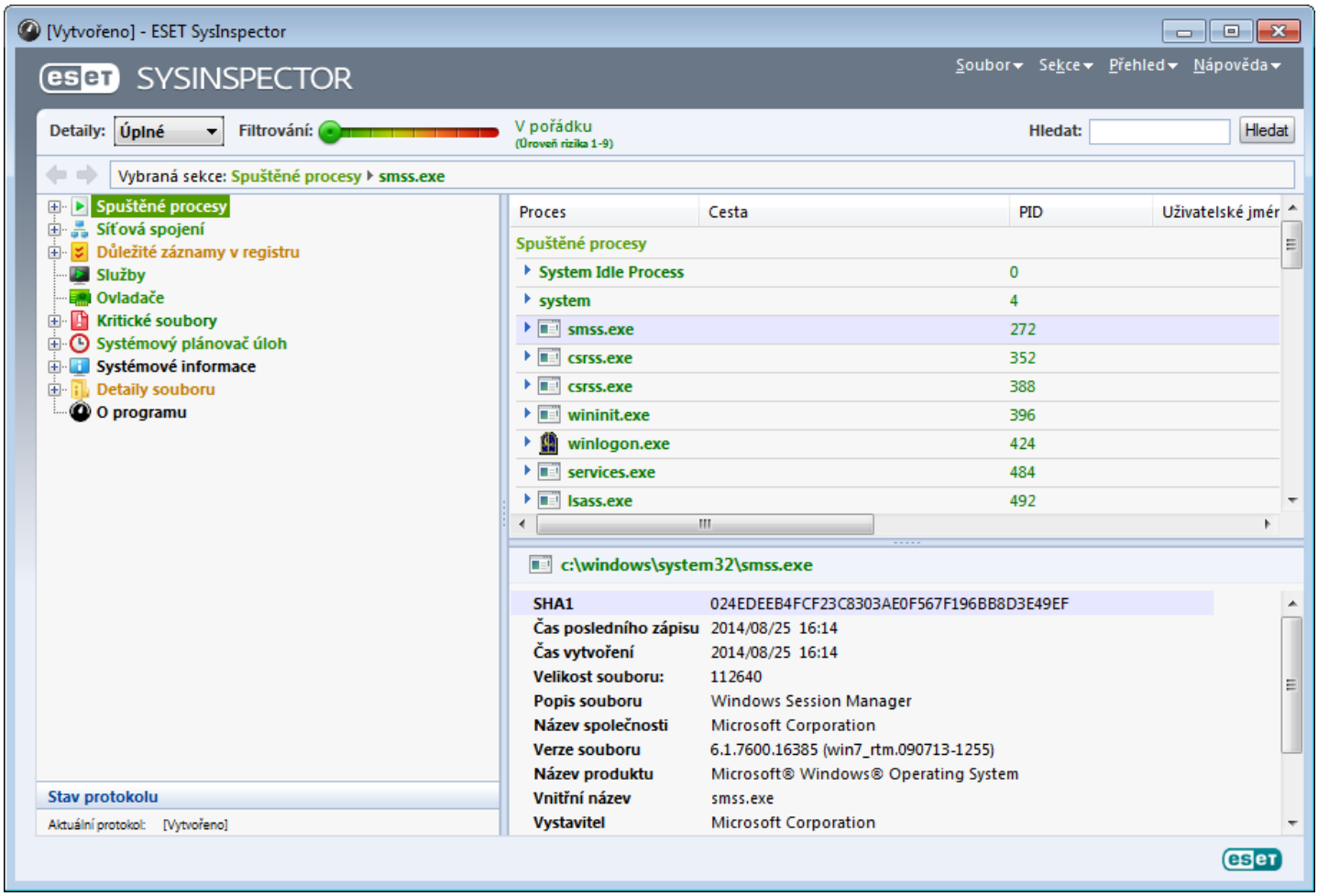
5.6.1.1 Spuštění programu ESET SysInspector

Pro spuštění programu ESET SysInspector klikněte na soubor *SysInspector.exe*, který jste stáhli z webových stránek společnosti ESET. Pokud již máte nainstalováno ESET Security řešení, můžete spustit ESET SysInspector přímo z Nabídky Start kliknutím na **Všechny programy** > **ESET** > **ESET Smart Security**).

Následně vyčkejte, dokud aplikace neprovede inspekci systému, což může trvat několik minut.

5.6.2 Uživatelské rozhraní a používání aplikace

Pro snadné používání je hlavní okno rozděleno do čtyř hlavních sekcí – **Ovládání programu** je umístěno v horní části hlavního okna, **Navigační okno** naleznete vlevo a **Okno s popisem** vpravo ve střední části. **Okno s detaily** se nachází v pravé části dole. Sekce **Stav protokolu** zobrazuje základní parametry protokolu (použitý filtr, typ filtru, zda je protokol výsledkem srovnání atd.).



5.6.2.1 Ovládací prvky programu

Tato sekce obsahuje popis všech ovládacích prvků dostupných v programu ESET SysInspector.

Soubor

Kliknutím na **Soubor** můžete uložit současný protokol pro pozdější prozkoumání, nebo otevřít dříve uložený protokol. Pokud chcete protokol zveřejnit, doporučujeme jej vygenerovat jako vhodný **Připravený k odeslání** (CTRL + G). V tomto případě se vynechají citlivé informace (uživatelské jméno, název počítače, oprávnění uživatele, proměnné prostředí atd.).

Poznámka: Uložené protokoly programu ESET SysInspector můžete jednoduše otevřít přetažením .xml souboru do hlavního okna.

Sekce

Umožňuje rozbalit nebo zavřít všechny sekce a exportovat vybrané části do Servisního skriptu.

Přehled

Obsahuje funkce pro snadnější navigaci v programu a další funkce, jako například vyhledávání informací online.

Nápověda

Obsahuje informace o aplikaci a dostupných funkcích.

Detaily

Toto nastavení ovlivňuje informace zobrazené v ostatních sekcích hlavního okna. V "Základním" režimu máte přístup k informacím, které se používají k nalezení běžných problémů. Ve "Středním" režimu program zobrazuje i méně používané detaily, zatímco v "Úplném" režimu ESET SysInspector zobrazí všechny informace potřebné k vyřešení specifických problémů.

Filtrování

Slouží k vyhledání podezřelých souborů nebo záznamů v systémovém registru. Nastavením posuvníku můžete filtrovat položky podle jejich úrovně rizika. Pokud je posuvník nastaven co nejvíce vlevo (Úroveň ohrožení 1), jsou zobrazeny všechny položky. Nastavením posuvníku více doprava odfiltrujete všechny položky s menší mírou rizika. Pokud je posuvník nastaven co nejvíce vpravo, program zobrazí pouze známé škodlivé položky.

Všechny položky, které mají úroveň rizika 6 až 9 mohou představovat bezpečnostní riziko. Pokud nepoužíváte bezpečnostní řešení od společnosti ESET a ESET SysInspector detekoval nebezpečné záznamy, doporučujeme zkontrolovat systém pomocí ESET Online Scanner. ESET Online Scanner je služba dostupná zdarma.

Poznámka: Úroveň rizika položky se dá rychle určit porovnáním barvy dané položky s barvou na posuvníku úrovně rizika.

Porovnat

Při porovnávání dvou protokolů můžete zobrazit všechny záznamy, pouze nově přidané nebo naopak odebrané případně nahrazené záznamy.

Hledat

Vyhledávání můžete použít pro rychlé vyhledání celého názvu záznamu nebo pouze jeho části. Výsledky vyhledávání se zobrazí v okně s detaily.

Zpět

Kliknutím na šipku zpět nebo vpřed se můžete vrátit k předchozí zobrazené informaci v okně s detaily. Místo klikání na šipky můžete použít klávesy backspace a mezerník.

Zobrazená sekce

Zobrazuje současnou sekci v navigačním okně.

Důležité: Položky označené červenou barvou jsou neznámé, proto je program označí jako potenciálně nebezpečné. Pokud je některá položka červená, neznamená to, že můžete automaticky daný soubor vymazat. Před samotným vymazáním se ujistěte, že jsou soubory skutečně nebezpečné nebo nepotřebné.

5.6.2.2 Navigace v programu ESET SysInspector

ESET SysInspector rozděluje několik typů informací do několika základních sekcí, které se nazývají uzly. Případně podrobnější informaci získáte rozbalením jednotlivých uzlů a zobrazením poduzlů. Pro rozbalení nebo zavření uzlu, dvakrát poklepejte na název nebo klikněte na + nebo − vedle názvu uzlu. Při prohlížení stromové struktury uzlů a poduzlů v navigačním okně více detailů pro každý uzel naleznete v okně s popisem. Pokud prohlížíte položky v okně s popisem, další detaily pro každý typ položky mohou být zobrazeny v okně s detaily.

Následují popisy hlavních uzlů v navigačním okně a související informace v oknech popisem a detaily.

Spuštěné procesy

Tato větev obsahuje informace o aplikacích a procesech, které jsou spuštěny v době generování protokolu. V okně Popis můžete najít další informace pro každý proces, jako které knihovny proces používá a jejich umístění v systému, jméno výrobce aplikace a úroveň rizika daného souboru.

Okno Detaily obsahuje další informace o vybraných položkách v okně Popis, jako například velikost souboru, nebo jeho kontrolní součet.

Poznámka: Operační systém se skládá z několika důležitých komponent jádra systému, které běží nepřetržitě a

poskytují základní funkce pro ostatní uživatelské aplikace. V některých případech jsou tyto procesy zobrazeny v protokolu ESET SysInspector s cestou začínající na \??\. Tyto symboly poskytují optimalizaci ještě před spuštěním pro těchto procesů; jsou bezpečné pro systém.

Síťová připojení

Okno Popis obsahuje seznam procesů a aplikací, které komunikují přes síť pomocí protokolu, který je vybrán v navigačním okně (TCP nebo UDP) a také vzdálenou adresu, kam se daná aplikace připojuje. Také můžete zkontrolovat IP adresy DNS serverů.

Okno Detaily obsahuje další informace o vybraných položkách v okně Popis, jako například velikost souboru, nebo jeho kontrolní součet.

Důležité záznamy v registru

Obsahuje seznam vybraných položek registru Windows, které často souvisí s různými problémy, například ty, které definují programy spouštěny po startu, browser helper objects (BHO) atd.

V okně Popis můžete zjistit, které soubory souvisí s konkrétními položkami v registru. Další informace se zobrazí v okně Detaily.

Služby

Okno Popis obsahuje seznam souborů, které jsou zaregistrovány jako služby systému Windows. Můžete si zkontrolovat, jakým způsobem se služba spouští společně se specifickými parametry souboru v okně s Detaily.

Ovladače

Seznam instalovaných ovladačů v systému.

Kritické soubory

V okně Popis se zobrazí kritické soubory spojené s operačním systémem Microsoft Windows.

Systémový plánovač úloh

Obsahuje seznam úloh naplánovaných pomocí Plánovače úloh Windows.

Systémové informace

Obsahuje detailní informace o hardwaru a softwaru společně s informacemi o nastavených globálních proměnných, uživatelských právech a systémových protokolech událostí.

Detaily souboru

Seznam důležitých systémových souborů a souborů ve složce Program Files. Další informace specifické pro soubory naleznete v oknech Popis a Detaily.

O programu

Informace o programu ESET SysInspector a seznam modulů programu.

5.6.2.2.1 Klávesové zkratky

Klávesové zkratky, které můžete použít při práci s programem ESET SysInspector.

Soubor

Ctrl+O	otevře existující protokol
Ctrl+S	uloží vytvořený protokol

Analýza systému

Ctrl+G	vytvoří standardní záznam o počítači
Ctrl+H	vytvoří záznam o počítači, který může obsahovat citlivé informace

Filtrování položek

1, O	v pořádku, jsou zobrazeny položky s úrovní rizika 1-9
2	v pořádku, jsou zobrazeny položky s úrovní rizika 2-9
3	v pořádku, jsou zobrazeny položky s úrovní rizika 3-9
4, U	neznámé, jsou zobrazeny položky s úrovní rizika 4-9
5	neznámé, jsou zobrazeny položky s úrovní rizika 5-9
6	neznámé, jsou zobrazeny položky s úrovní rizika 6-9
7, B	nebezpečné, jsou zobrazeny položky s úrovní rizika 7-9
8	nebezpečné, jsou zobrazeny položky s úrovní rizika 8-9
9	nebezpečné, jsou zobrazeny položky s úrovní rizika 9
-	snižuje úroveň rizika
+	zvyšuje úroveň rizika
Ctrl+9	režim filtrování, stejná úroveň nebo vyšší
Ctrl+0	režim filtrování, pouze stejná úroveň

Zobrazit

Ctrl+5	zobrazit podle výrobce, všichni výrobci
Ctrl+6	zobrazit podle výrobce, pouze Microsoft
Ctrl+7	zobrazit podle výrobce, všichni ostatní výrobci
Ctrl+3	zobrazí úplné detaily
Ctrl+2	zobrazí střední detaily
Ctrl+1	základní zobrazení
BackSpace	krok zpět
Mezerník	krok vpřed
Ctrl+W	rozbalí stromovou strukturu
Ctrl+Q	sbalí stromovou strukturu

Další

Ctrl+T	přejde na původní umístění položky po vyjmutí ve výsledcích vyhledávání
Ctrl+P	zobrazí základní informace o položce
Ctrl+A	zobrazí úplné informace o položce
Ctrl+C	zkopíruje stromovou větev aktuální položky
Ctrl+X	zkopíruje všechny položky
Ctrl+B	vyhledá informace o vybrané položce na internetu
Ctrl+L	otevře složku, kde se nachází vybraný soubor
Ctrl+R	otevře odpovídající záznam v Editoru registru
Ctrl+Z	zkopíruje cestu k souboru (pokud označena položka souvisí se souborem)
Ctrl+F	přepne se do vyhledávacího pole
Ctrl+D	zavře výsledky vyhledávání
Ctrl+E	spustí servisní skript

Porovnání

Ctrl+Alt+O	otevře protokol k porovnání
Ctrl+Alt+R	zruší porovnání
Ctrl+Alt+1	zobrazí všechny položky
Ctrl+Alt+2	zobrazí pouze přidané položky, tedy položky, které jsou přítomny v aktuálním protokolu
Ctrl+Alt+3	zobrazí pouze odebrané položky, tedy položky, které jsou přítomny v předchozím protokolu
Ctrl+Alt+4	zobrazí pouze nahrazené položky (včetně souborů)
Ctrl+Alt+5	zobrazí pouze rozdíly mezi protokoly
Ctrl+Alt+C	zobrazí porovnání
Ctrl+Alt+N	otevře aktuální protokol
Ctrl+Alt+P	otevře předchozí protokol

Různé

F1	zobrazí nápovědu

Alt+F4	zavře program
Alt+Shift+F4	zavře program bez dotazu
Ctrl+I	statistiky protokolu

5.6.2.3 Porovnávání

Funkce porovnání umožňuje porovnat dva stávající protokoly. Výstupem této funkce je sada záznamů, které nejsou společné pro oba protokoly. To je vhodné ve chvíli, kdy chcete sledovat změny v systému a užitečné také při detekci škodlivého programu.

Po spuštění programu ESET SysInspector se vytvoří nový protokol a zobrazí v novém okně. Pro otevření již existujícího protokolu použijte menu **Soubor** > **Otevřít protokol**. V hlavním okně programu se vždy zobrazí zároveň pouze jeden protokol.

Pokud porovnáváte dva protokoly, princip spočívá v tom, že porovnáváte právě aktivní protokol s protokolem uloženým v souboru. Pro porovnání protokolů klikněte na **Soubor** > **Porovnat protokoly** a vyberte **Vybrat soubor**. Vybraný protokol bude porovnán s aktivním v hlavním okně programu. Výsledný tzv. srovnávací protokol zobrazí pouze rozdíly mezi těmito dvěma protokoly.

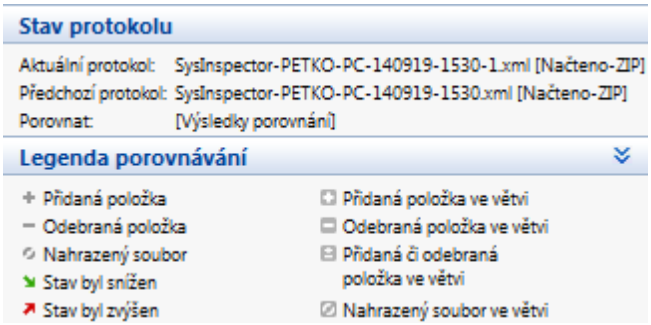
Poznámka: V případě, že porovnáváte dva protokoly, kliknutím na **Soubor** > **Uložit protokol** uložíte oba soubory jako ZIP archiv. Pokud později tento archiv otevřete, protokoly v něm obsažené, budou automaticky porovnány.

Vedle zobrazených položek ESET SysInspector zobrazuje symboly identifikující rozdíly mezi porovnávanými protokoly.

Význam jednotlivých symbolů:

- + nová hodnota, nebyla přítomna v předchozím protokolu
- sekce se stromovou strukturou obsahuje nové hodnoty
- – odebraná hodnota, přítomna pouze v předchozím protokolu
- sekce se stromovou strukturou obsahuje odebrané hodnoty
- hodnota/soubor byly změněny
- sekce se stromovou strukturou obsahuje změněné hodnoty/soubory
- úroveň rizika klesla/byla vyšší v předchozím protokolu
- úroveň rizika vzrostla/byla nižší v předchozím protokolu

Vysvětlující sekce v levém dolním rohu popisuje všechny symboly a také zobrazuje názvy protokolů, které jsou porovnávány.



Kterýkoli srovnávací protokol může být uložen do souboru a kdykoliv později otevřen.

Příklad

Vygenerujte a uložte protokol, který zaznamená původní informace o systému do souboru puvodni.xml. Poté, co budou provedeny změny v systému otevřete ESET SysInspector a vygenerujte nový protokol, který uložte do souboru aktualni.xml.

Pro zjištění změn mezi těmito dvěma protokoly klikněte na **Soubor** > **Porovnat protokoly**. Program vytvoří srovnávací protokol a zobrazí rozdíly mezi protokoly.

Stejného výsledku dosáhnete, pokud zadáte následující příkaz do příkazového řádku:

SysIsnpector.exe aktualni.xml puvodni.xml

5.6.3 Ovládaní prostřednictvím příkazového řádku

ESET SysInspector podporuje generování protokolů z příkazového řádku za použití následujících parametrů:

/gen	vygeneruje protokol přímo z příkazové řádky bez spuštění grafického rozhraní
/privacy	vygeneruje protokol bez citlivých informací
/zip	uloží výsledný protokol přímo na disk v zip archivu
/silent	tento parametr potlačí zobrazení ukazatele průběhu při generování protokolu
/blank	spustí ESET SysInspector bez vytvoření/načtení protokolu

Příklady

Použití:

```
Sysinspector.exe [puvodni.xml] [/gen=novy.xml] [/privacy] [/zip] [srovnani.xml]
```

Pro zobrazení specifického protokolu v prohlížeči použijte: *SysInspector.exe .\protokol.xml*
Pro vygenerování protokolu použijte: *SysInspector.exe /gen=.\novyprotokol.xml*
Pro vygenerování protokolu bez citlivých informací použijte: *SysInspector.exe /gen=.\novyprotokol.zip /privacy /zip*
Pro porovnání dvou protokolů použijte: *SysInspector.exe "novy.xml" "puvodni.xml"*

Poznámka: Pokud název souboru nebo složky obsahuje mezeru, měl by být zadán s uvozovkami.

5.6.4 Servisní skript

Servisní skript je nástroj, který umožňuje pomocí ESET SysInspector odstranit nežádoucí objekty ze systému.

Servisní skript umožňuje exportovat celý ESET SysInspector protokol, nebo pouze vybrané části. Po exportování můžete označit nežádoucí objekty, které chcete odstranit. Poté stačí upravený protokol spustit a dojde k odstranění označených objektů.

Servisní skript je určen pokročilým uživatelům s předchozími zkušenostmi v diagnostice systémových problémů. Neodborné zásahy mohou vést k poškození operačního systému.

Příklad

Pokud máte podezření, že je počítač napaden virem, který není detekován antivirovým programem, pokračujte podle následujících kroků:

1. Spusťte ESET SysInspector a vygenerujte nový protokol o systému.
2. Vyberte první položku v sekci nalevo (ve stromové struktuře), stiskněte klávesu **Shift** a vyberte poslední položku pro označení všech položek.
3. Klikněte pravým tlačítkem myši na označené objekty a vyberte z kontextového menu možnost **Exportovat vybrané sekce do Servisního skriptu**.
4. Vybrané objekty budou vyexportovány do nového souboru.
5. Toto je nejdůležitější krok v celém procesu: otevřete uložený soubor v Poznámkovém bloku a změňte atribut - na + u všech objektů, které chcete odstranit. Ujistěte se, že jste neoznačili žádné objekty, které jsou nezbytné pro správné fungování systému.
6. Spusťte ESET SysInspector, klikněte na **Soubor** > **Spustit servisní skript** a zadejte cestu k upravenému skriptu.
7. Klikněte na **OK** pro spuštění skriptu.

5.6.4.1 Generování servisního skriptu

Pro vygenerování skriptu, klikněte pravým tlačítkem myši na libovolnou položku ve stromové struktuře (v levé části) v hlavním okně programu ESET SysInspector. Z kontextového menu vyberte možnost **Exportovat všechny sekce do Servisního skriptu** nebo **Exportovat vybrané sekce do Servisního skriptu**.

Poznámka: Není možné exportovat servisní skript, pokud se porovnávají dva protokoly.

5.6.4.2 Struktura servisního skriptu

V prvním řádku hlavičky skriptu se nacházejí informace o verzi enginu (ev), verzi grafického rozhraní (gv) a verzi protokolu (lv). Tato data můžete použít při hledání možných změn v .xml souboru, které generuje skript a zamezit veškerým nesrovnalostem během provádění skriptu. Tato část skriptu by neměla být modifikována.

Zbytek souboru je rozdělen do sekcí, ve kterých můžete jednotlivé položky modifikovat (označit ty, které budou zpracovány skriptem). Položky ke zpracování označíte tak, že zaměníte znak "-" před položkou za znak "+". Jednotlivé sekce ve skriptu jsou odděleny prázdným řádkem. Každá sekce má číslo a nadpis.

01) Running processes

Tato sekce obsahuje seznam všech běžících procesů v systému. Každý proces je identifikován svou UNC cestou a následně kontrolním součtem CRC16 mezi hvězdičkami (*).

Příklad:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

V tomto příkladu byl vybrán proces module32.exe (označen znakem "+"); proces bude ukončen při spuštění skriptu.

02) Loaded modules

Tato sekce obsahuje seznam aktuálně použitých systémových modulů.

Příklad:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

V tomto příkladu byl modul khbekhb.dll označen znakem "+". Když se skript spustí, rozpozná procesy, které používají tento specifický modul a ukončí je.

03) TCP connections

Tato sekce obsahuje informace o existujících TCP spojeních.

Příklad:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

Když se skript spustí, najde vlastníka socketu v označených TCP spojeních a zastaví tento socket, čímž uvolní systémové prostředky.

04) UDP endpoints

Tato sekce obsahuje informace o stávajících koncových bodech UDP.

Příklad:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Když se skript spustí, izoluje vlastníka socketu v označených koncových bodech UDP a zastaví tento socket.

05) DNS server entries

Tato sekce obsahuje informace o současné konfiguraci DNS serverů.

Příklad:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Označené záznamy DNS budou odstraněny.

06) Important registry entries

Tato sekce obsahuje informace o důležitých záznamech v registru Windows.

Příklad:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Označené hodnoty budou po spuštění skriptu vymazány, redukovány na 0 bajtové hodnoty, nebo vynulovány na základních hodnoty. Akce, která se provede po spuštění skriptu, závisí na kategorii dané položky a hodnotě klíče v konkrétní větvi registru.

07) Services

Tato sekce obsahuje seznam služeb zaregistrovaných v systému.

Příklad:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

Označené služby a služby na nich závislé budou po spuštění skriptu zastaveny a odinstalovány.

08) Drivers

Tato sekce obsahuje seznam nainstalovaných ovladačů.

Příklad:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Po spuštění skriptu budou vybrané ovladače odregistrovány ze systému a následně odstraněny.

09) Critical files

Tato sekce obsahuje informace o souborech, které jsou kritické pro správné fungování operačního systému.

Příklad:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Vybrané položky budou odstraněny nebo vynulovány na své původní hodnoty.

10) Scheduled tasks

Tato sekce obsahuje informace o naplánovaných úlohách.

Příklad:

```
10) Scheduled tasks
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe /c
- c:\users\admin\appdata\local\google\update\googleupdate.exe /ua /installsource
- %windir%\system32\appidpolicyconverter.exe
- %windir%\system32\appidcertstorecheck.exe
- aitagent
[...]
```

5.6.4.3 Spouštění servisních skriptů

Označte všechny požadované položky, poté skript uložte a zavřete. Spusťte změněný skript přímo z hlavního okna programu ESET SysInspector vybráním možnosti **Spustit servisní skript** z menu **Soubor**. Když otevřete skript, program zobrazí následující upozornění: **Opravdu chcete spustit Servisní skript "%Scriptname%"?** Po potvrzení této akce se může objevit další upozornění s informací, že servisní skript, který se pokoušíte spustit, nebyl podepsán. Klikněte na **Spustit** pro spuštění skriptu.

Zobrazí se dialogové okno s informací o úspěšném provedení skriptu.

Pokud byl skript zpracován pouze z části, objeví se dialogové okno s následující zprávou: **Servisní skript byl spuštěn pouze částečně. Chcete zobrazit chybové hlášení?** Klikněte na **Ano** pro zobrazení úplného chybového protokolu se seznamem operací, které nebyly provedeny.

Pokud nebyl skript rozpoznán, zobrazí se dialogové okno s následující zprávou: **Vybraný Servisní skript není podepsán. Spuštění nepodepsaných a neznámých skriptů může vážně poškodit vaše data v počítači. Jste si jisti, že chcete Spustit skript a provést akci?** Toto může být způsobeno nesrovnalostmi ve skriptu (poškozená hlavička,

poškozený nadpis sekce, chybějící prázdný řádek mezi dvěma sekcemi atd.). V takovém případě znovu otevřete servisní skript a opravte chyby nebo vytvořte skript nový.

5.6.5 Často kladené otázky

Potřebuje ke svému běhu ESET SysInspector oprávnění Administrátora?

ESET SysInspector nepotřebuje pro spuštění oprávnění Administrátora, ale některé informace, které sbírá, jsou přístupné pouze pro administrátorský účet. Spuštění programu jako Standardní uživatel nebo Uživatel s omezeným oprávněním bude mít za následek shromáždění méně informací o operačním prostředí.

Vytváří ESET SysInspector soubor s protokolem?

ESET SysInspector dokáže vytvořit soubor s protokolem o konfiguraci počítače. Pro uložení souboru klikněte v hlavním menu na **Soubor** > **Uložit protokol**. Protokoly jsou ukládány v XML formátu, standardně do složky *%uživatel%\Dokumenty* s názvem souboru podle konvence "SysInspector-%NÁZEVPOČÍTAČE%-RRMMDD-HHMM.XML". Umístění a název protokolu můžete před uložením změnit, pokud si to přejete.

Jak si prohlédnu protokol ESET SysInspector?

Pro zobrazení protokolu, který vytvořil ESET SysInspector, spusťte program a klikněte v hlavním menu na **Soubor** > **Načíst protokol**. Můžete také soubor přetáhnout do okna programu ESET SysInspector. Pokud si potřebujete často prohlížet protokoly programu ESET SysInspector, doporučujeme vytvořit na Ploše zástupce souboru *SysInspector.exe*; poté můžete protokoly prohlížet pouhým přetažením souboru na vytvořeného zástupce. Z bezpečnostních důvodů nemusí Windows Vista/7 povolit přetahování souboru mezi okny, která mají různá bezpečnostní práva.

Je k dispozici specifikace formátu souboru s protokolem? Co SDK?

V současnosti není k dispozici ani specifikace, ani SDK, protože program je stále ve vývoji. Poté, co bude program uvolněn, můžeme tyto informace poskytnout na základě zpětné vazby a požadavků uživatelů.

Jak ESET SysInspector vyhodnotí riziko, které představuje konkrétní objekt?

Většinou ESET SysInspector přiřadí úroveň rizika objektům (soubory, procesy, klíče v registru atd.) použitím série heuristických pravidel, kterými ověří charakteristiku každého objektu, a poté zváží potenciál pro škodlivou činnost. Na základě této heuristiky se objektu přiřadí úroveň rizika od 1 - V pořádku (zelená) do 9 - Nebezpečné (červená). V levém navigačním okně jsou jednotlivé sekce zabarvené barvou podle objektu s nejvyšší úrovní rizika, který se v nich nachází.

Znamená úroveň rizika "6 - Neznámé (červená)," že je objekt nebezpečný?

Odhad programu ESET SysInspector nezaručuje, že je objekt škodlivý – toto rozhodnutí by měl udělat bezpečnostní expert.ESET SysInspector je navržen pro poskytnutí rychlého souhrnu, na které objekty se má bezpečnostní expert zaměřit pro podrobnější zkoumání neobvyklého chování.

Proč se ESET SysInspector po spuštění připojuje k internetu?

Jako mnoho jiných aplikací, také ESET SysInspector je podepsán digitálním certifikátem, aby bylo možné zaručit, že software byl vydán společností ESET a nebyl modifikován. Pro ověření daného certifikátu operační systém kontaktuje certifikační autoritu pro ověření identity vydavatele softwaru. Toto je normální chování pro všechny digitálně podepsané programy pod operačním systémem Microsoft Windows.

Co je technologie Anti-Stealth ?

Technologie Anti-Stealth poskytuje efektivní detekci rootkitů.

Pokud je systém napaden škodlivým kódem, který se chová jako rootkit, uživatel může být vystaven riziku poškození, ztráty nebo odcizení dat. Bez speciálních anti-rootkit nástrojů je téměř nemožné detekovat rootkity.

Proč jsou někdy soubory označené jako "Podepsal Microsoft" a zároveň mají jiné "Jméno společnosti"?

Při pokusu identifikovat digitální podpis spustitelného souboru SysInspector nejdříve hledá digitální podpis vložený

v souboru. Pokud jej najde, pro ověření se použije tato identifikace. Na druhé straně, pokud soubor neobsahuje digitální podpis, ESI začne hledat příslušný CAT soubor (Security Catalog - *%systemroot%\system32\CatRoot*), který obsahuje informace o zpracovávaném spustitelném souboru. V případě, že se najde patřičný CAT soubor, digitální podpis toho CAT souboru se použije při ověřovacím procesu spustitelného souboru.

Toto je důvod, proč jsou někdy soubory označené jako "Podepsal Microsoft" a zároveň mají jiné "Jméno společnosti."

Příklad:

Windows 2000 obsahuje aplikaci HyperTerminal umístěnou v *C:\Program Files\Windows NT*. Hlavní spustitelný soubor aplikace není digitálně podepsán, ale SysInspector soubor označí jako podepsaný společností Microsoft. Důvodem je reference v *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* odkazující na *C:\Program Files\Windows NT\hypertrm.exe* (hlavní spustitelný soubor aplikace HyperTerminal) a sp4.cat, který je digitálně podepsán společností Microsoft.

5.6.6 ESET SysInspector jako součást ESET Smart Security

ESET SysInspector můžete také otevřít přímo v ESET Smart Security kliknutím na záložku **Nástroje** > **ESET SysInspector**. Okno správy ESET SysInspector je velmi podobné protokolům a plánovači úloh. Všechny operace – vytvoření, prohlížení, porovnávání, odstranění a export protokolu – jsou dostupné pomocí jednoho nebo dvou kliknutí myší.

Okno ESET SysInspector obsahuje základní informace o vytvořených záznamech jako je čas vytvoření, krátký komentář, jméno uživatele a stav.

Pro porovnání, vytvoření nebo odstranění protokolu použijte příslušná tlačítka umístěná v dolní části okna ESET SysInspector. Tyto možnosti jsou také dostupné z kontextového menu, které dále obsahuje možnost **Zobrazit**. Pro exportování vybraných protokolů klikněte pravým tlačítkem myši a vyberte možnost **Exportovat...**.

Podrobný popis funkcí:

- **Porovnat** – umožňuje porovnat dva existující protokoly. To je vhodné, pokud potřebujete identifikovat změny ve stávajícím a předchozím protokolu. Pro tuto možnost musíte ze seznamu vybrat 2 záznamy.
- **Přidat...** – vytvoří nový záznam. Před vytvořením musíte zadat krátký komentář o záznamu. Pro zjištění průběhu vytváření protokolu se podívejte do sloupce **Stav**. Všechny vytvořené protokoly mají stav **Vytvořeno**.
- **Odstranit/Odstranit vše** – odstraní záznamy ze seznamu.
- **Exportovat...** – uloží protokol do XML souboru (také jako zip archiv).

5.7 Příkazový řádek

Antivirový modul ESET Smart Security můžete spustit pomocí příkazového řádku – ručně (příkazem "ecls") nebo dávkovým souborem typu "bat". Použití ESET skenovacího modulu z příkazového řádku:

```
ecls [MOŽNOSTI..] SOUBORY..
```

Při spouštění kontroly na vyžádání přes příkazový řádek můžete použít několik parametrů a přepínačů:

Možnosti

/base-dir=SLOŽKA	načíst moduly ze SLOŽKY
/quar-dir=SLOŽKA	soubory ulož do karantény - SLOŽKY
/exclude=MASKA	vyloučí soubory odpovídající MASCE z kontroly
/subdir	zahrnout podsložky (standardně)
/no-subdir	nezahrnovat podsložky
/max-subdir-level=ÚROVEŇ	podsložky zkontrolovat pouze do hloubky ÚROVNĚ (standardně 0 = neomezeně)
/symlink	následovat symbolické odkazy (standardně)
/no-symlink	přeskočit symbolické odkazy
/ads	kontrolovat ADS (standardně)
/no-ads	nekontrolovat ADS
/log-file=SOUBOR	zapisovat výstup do SOUBORU
/log-rewrite	přepisovat výstupní soubor (standardně se přidá na konec současného)
/log-console	zapisovat výstup na konzoli

/no-log-console	nezapisovat výstup na konzoli
/log-all	vypsat i čisté soubory
/no-log-all	nevypisovat čisté soubory (standardně)
/aind	zobrazit indikátor aktivity
/auto	automaticky zkontrolovat a vyléčit všechny lokální disky

Možnosti skeneru

/files	kontrolovat soubory (standardně)
/no-files	nekontrolovat soubory
/memory	kontrolovat paměť
/boots	kontrolovat zaváděcí sektory
/no-boots	nekontrolovat zaváděcí sektory (standardně)
/arch	kontrolovat archivy (standardně)
/no-arch	nekontrolovat archivy
/max-obj-size=VELIKOST	kontrolovat pouze soubory menší než VELIKOST megabajtů (standardně 0 = neomezené)
/max-arch-level=ÚROVEŇ	archivy kontrolovat do hloubky ÚROVNĚ
/scan-timeout=LIMIT	archivy kontrolovat nejdéle LIMIT sekund
/max-arch-size=VELIKOST	kontrolovat pouze soubory v archivech menší než VELIKOST megabajtů (standardně 0 = neomezené)
/max-sfx-size=VELIKOST	kontrolovat pouze soubory v samorozbalovacích archivech menší než VELIKOST megabajtů (standardně 0 = neomezené)
/mail	kontrolovat poštovní soubory (standardně)
/no-mail	nekontrolovat poštovní soubory
/mailbox	kontrolovat poštovní schránky (standardně)
/no-mailbox	nekontrolovat poštovní schránky
/sfx	kontrolovat samorozbalovací archivy (standardně)
/no-sfx	nekontrolovat samorozbalovací archivy
/rtp	kontrolovat runtime archivy (standardně)
/no-rtp	nekontrolovat runtime archivy
/adware	kontrolovat adware aplikace (standardně)
/no-adware	nekontrolovat adware aplikace
/unsafe	kontrolovat zneužitelné aplikace
/no-unsafe	nekontrolovat zneužitelné aplikace (standardně)
/unwanted	kontrolovat nechtěné aplikace
/no-unwanted	nekontrolovat nechtěné aplikace (standardně)
/pattern	použít vzorky (standardně)
/no-pattern	nepoužívat vzorky
/heur	zapnout heuristiku (standardně)
/no-heur	vypnout heuristiku
/adv-heur	zapnout rozšířenou heuristiku (standardně)
/no-adv-heur	vypnout rozšířenou heuristiku
/ext=PŘÍPONY	kontrolovat pouze dvojtečkou oddělené PŘÍPONY
/ext-exclude=PŘÍPONY	vyloučit z kontroly dvojtečkou oddělené PŘÍPONY
/clean-mode=REŽIM	použít REŽIM léčení infikovaných objektů: none, standard (výchozí), strict, rigorous, delete
/quarantine	uložit infikované soubory (při léčení) do karantény (kromě vykonání AKCE)
/no-quarantine	neukládat infikované soubory do karantény

Všeobecné volby

/help	zobrazit tuto pomůcku a skončit
/version	zobrazit informaci o verzi a skončit
/preserve-time	zachovat čas přístupu k souborům

Návratové hodnoty

0	nenalezena žádná infekce

1	infekce nalezena a odstraněna
10	některé soubory nemohly být zkontrolovány (mohou obsahovat infekci)
50	nalezena infekce
100	chyba

Poznámka: Návratové hodnoty větší než 100 znamenají, že soubor nebyl zkontrolován a může být infikován.

6. Slovník pojmů

6.1 Typy infiltrací

Jako infiltrace je označován škodlivý software, který se snaží proniknout do počítače a vykonávat škodlivou činnost.

6.1.1 Viry

Tento druh infiltrací obvykle napadá již existující soubory na disku. Pojmenován byl podle biologického viru, protože se z počítače na další počítač šíří obdobným způsobem. Pojem vir se často nesprávně používá pro označení dalších typů hrozeb a infiltrací. Tento zaběhnutý výraz dnes nahrazuje mnohem přesnější termín "malware" (škodlivý software).

Počítačové viry napadají nejčastěji spustitelné soubory a dokumenty. Děje se to tak, že „tělo“ viru se k nim připojí – obvykle na konec souboru. Průběh aktivace počítačového viru je tedy zhruba následující: po spuštění napadeného souboru nejprve dojde ke spuštění připojeného viru. Ten vykoná akci, kterou má v sobě naprogramovanou. A až nakonec se ke slovu dostane původní aplikace. Vir může nakazit každý soubor, ke kterému má aktuálně přihlášený uživatel oprávnění pro zápis.

Vlastní činnost aktivovaného viru může mít mnoho podob. Některé viry jsou krajně nebezpečné, protože dokáží cíleně mazat soubory z disku, na druhé straně jiné mají pouze zdůraznit zručnost svých tvůrců a uživatele spíše obtěžují, než aby způsobovaly reálnou škodu.

V případě infikování virem není možné napadený soubor vrátit do původní podoby, tedy vyléčit jej pomocí antivirového systému. V některých případech není možné části infikovaných souborů vyléčit a musí být nahrazeny pouze čistou kopií. Přesto jej doporučujeme odeslat do virových laboratoří společnosti ESET.

6.1.2 Červi

Počítačový červ je program obsahující škodlivý kód, který napadá hostitelské počítače a šíří se dál prostřednictvím sítě. Základní rozdíl mezi virem a červem je ten, že červ se dokáže šířit sám a není závislý na hostitelském souboru (či boot sektoru disku). Červ využívá k šíření hlavně elektronickou poštou nebo bezpečnostní zranitelnosti v síťových aplikacích.

Červ je tedy mnohem životaschopnější než virus. Díky značnému rozšíření internetu se červ dokáže dostat do celého světa během několika hodin od vydání, v některých případech dokonce v průběhu několika minut – a proto je mnohem nebezpečnější než ostatní druhy malware.

Aktivovaný červ v systému dokáže způsobit celou řadu nepříjemností – od mazání souborů, přes značné zpomalení činnosti počítače, až po deaktivaci některých programů. Díky svému charakteru je ideální pro distribuci dalších druhů infiltrací.

V případě nákazy počítače červem doporučujeme infikovaný soubor odstranit, protože obsahuje výhradně škodlivý kód.

6.1.3 Trojské koně

Dříve platilo, že trojské koně byly typem infiltrace, která se snažila maskovat za užitečné programy, aby si zajistili své spuštění uživatelem.

Dnes se jedná o obecný pojem a trojské koně dělí do mnoha kategorií. Mezi nejznámější patří:

- **Downloader** – škodlivý program, jehož úlohou je z internetu stahovat do systému další infiltrace,
- **Dropper** – tzv. nosič. Přenáší v sobě ukrytý další škodlivý software a ztěžuje tím jejich detekci antivirovými programy,
- **Backdoor** – tzv. zadní dvířka. Jedná se o program komunikující se vzdáleným útočníkem, který tak může získat přístup a kontrolu nad napadeným systémem,
- **Keylogger** – sleduje, jaké klávesy uživatel stisknul a odesílá informace vzdálenému útočníkovi,
- **Dialer** – připojuje se na zahraniční telefonní čísla, která jsou zpoplatněna vysokými částkami. Uživatel prakticky

nemá šanci zaregistrovat odpojení od svého poskytovatele připojení a vytvoření nového připojení do zahraničí. Reálnou škodu mohou tyto programy způsobit pouze uživatelům s vytáčeným připojením (tzv. dial-up).

Pokud v počítači detekujete trojský kůň, doporučujeme daný soubor vymazat, protože zpravidla neobsahuje prakticky nic jiného, než samotný škodlivý kód.

6.1.4 Rootkity

Rootkit je škodlivý kód, který umožňuje získat útočníkovi neomezený přístup k počítači. Po nákaze (obvykle využití zranitelnost v systému) využívají ke svému zamaskování systémové funkce. Vydávají se za systémové procesy, soubory a složky, nebo data v registru a z tohoto důvodu je velmi těžké rootkity detekovat standardními technikami.

Rootkity lze detekovat:

1. Když se snaží získat přístup do systému. V této chvíli ještě nejsou aktivní a většina antivirových programů eliminuje rootkity na této úrovni (za předpokladu, že virová databáze obsahuje definici nakaženého souboru).
2. Když se skrývají před běžnou kontrolou počítače. Jako uživatelé ESET Smart Security se můžete spolehnout na technologii Anti-Stealth, která aktivně detekuje a eliminuje rootkity.

6.1.5 Adware

Adware je zkratka termínu „advertising-supported software“. Do této kategorie patří programy, jejichž úkolem je zobrazovat reklamy. Adware obvykle sám otevře nové vyskakovací okno (tzv. pop-up okno) s reklamou v internetovém prohlížeči nebo změní nastavení výchozí domovské stránky v internetovém prohlížeči. Používají jej často výrobci volně šiřitelných (bezplatných) programů, aby si finančně zajistili vývoj vlastní, v mnoha případech užitečné aplikace.

Adware sám o sobě nebývá škodlivý, pouze uživatele obtěžuje. Nebezpečí spočívá v tom, že často provádí sledování uživatele, podobně jako spyware.

Pokud se rozhodnete používat volně šiřitelný software, doporučujeme věnovat průběhu instalace zvýšenou pozornost. Instalační program totiž často upozorňuje na to, že se spolu s daným programem nainstaluje také adware, a zpravidla máte možnost jeho instalaci zakázat.

Některé programy ovšem bez přídavného adware není možné nainstalovat nebo bude jejich funkce omezena. Z toho vyplývá, že adware se může do systému dostat „legální“ cestou, protože s tím uživatel souhlasí. Pozornost je tedy namístě. Infikovaný soubor neobsahuje v podstatě nic jiného než samotný škodlivý kód, proto v případě infekce doporučujeme soubor vymazat.

6.1.6 Spyware

Kategorie spyware zahrnuje programy, které odesílají informace bez vědomí uživatele. Odesílány jsou různé statistické informace, jako například seznam navštěvovaných internetových stránek, seznam e-mailových adres v adresáři nebo klávesy stisknuté uživatelem.

Tvůrci těchto programů argumentují tím, že se pouze snaží zjistit potřeby nebo zájmy uživatele, aby mohli uživatelům zobrazovat cílenou reklamu. Hranice zneužitelnosti je však v tomto případě velmi nejasná a nelze zaručit, že získané informace škodlivou aplikací nebudou v budoucnosti zneužity. Údaje získané spyware programy totiž mohou obsahovat různé bezpečnostní kódy, čísla bankovních účtů a další citlivá data. Spyware se šíří společně s některými volně šiřitelnými programy, aby si jejich autoři zajistili zdroj příjmu nebo nabídli zakoupení placené verze programu. Často jste o této skutečnosti informováni během instalace a máte možnost zakoupit si placenou verzi, která spyware neobsahuje.

Příkladem volně šiřitelného software obsahujícího spyware jsou hlavně klientské aplikace sítí P2P (peer-to-peer). Zvláštní podkategorií jsou programy, které se vydávají za antispyware, přičemž samy obsahují spyware – například *Spyfalcon, Spy Sheriff*.

Infikovaný soubor neobsahuje v podstatě nic jiného než samotný škodlivý kód, proto infikovaný soubor doporučujeme vymazat.

6.1.7 Packery

Packery jsou runtime samorozbalovací spustitelné soubory, které spojují několik druhů škodlivého kódu do jednoho balíčku.

Nejběžnější packery jsou UPX, PE_Compact, PKLite a ASPack. Stejný malware může být detekován odlišně, pokud je komprimován pomocí rozdílných metod. Packery navíc dokáží v průběhu času měnit své "podpisy" ve snaze vyhnout se detekci ze strany antivirových programů.

6.1.8 Potenciálně zneužitelné aplikace

Existuje řada legitimních programů, které za běžných podmínek zjednodušují například správu počítačových sítí. V nesprávných rukách však mohou být zneužity k nekalým účelům. Proto ESET Smart Security dokáže detekovat potenciální hrozby.

V převážné většině se jedná o komerční a legitimní software. Může jít například o aplikace pro zobrazení vzdálené pracovní plochy, programy pro dešifrování kódů a hesel nebo tzv. keyloggery (programy na monitorování stisknutých kláves).

Pokud v počítači zjistíte přítomnost zneužitelné aplikace, kterou jste si do systému neinstalovali, doporučujeme její výskyt konzultovat se správcem sítě nebo příslušnou aplikaci odstranit.

6.1.9 Potenciálně nechtěné aplikace

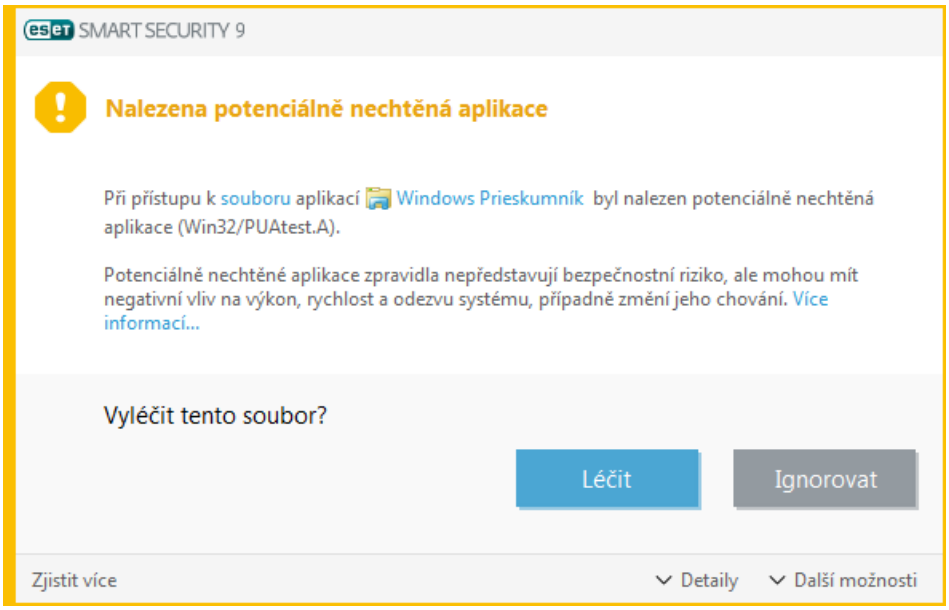
Potenciálně nechtěné aplikace jsou programy, které sice nemusí představovat bezpečnostní riziko, ale mohou mít negativní dopad na výkon počítače. Tyto aplikace se obvykle do systému nainstalují až po souhlasu uživatele. Jejich instalací dojde k určitým změnám v chování počítačového systému oproti stavu bez instalace příslušné aplikace. Mezi tyto změny v systému patří zejména:

- zobrazování oken (pop-up, reklamy), které by se jinak nezobrazovaly,
- aktivace a spuštění skrytých procesů,
- zvýšená spotřeba systémových prostředků,
- změny výsledků vyhledávání,
- komunikace se servery výrobce aplikace.

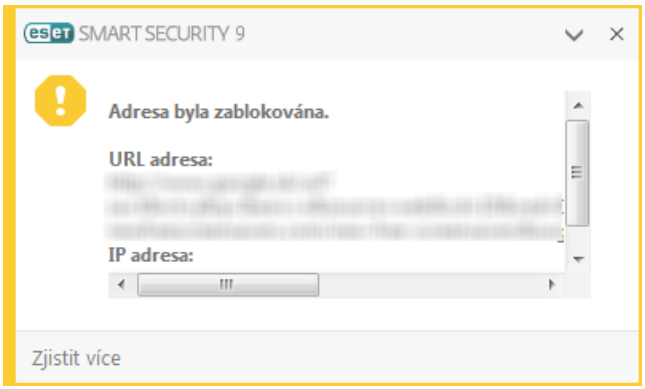
Varování - Nalezena potenciální hrozba

Při detekování potenciálně nechtěné aplikace se zobrazí dialogové okno s možností výběru akce:

1. **Vyléčit/Odpojit** – vybráním této možnosti zabráníte spuštění nebo stažení aplikace, a zabráníte tak infiltraci systému.
2. **Žádná akce** – po vybrání této možnosti se do vašeho systému dostane potenciální hrozba.
3. Pokud chcete danou aplikaci používat a nechcete aby vás produkt ESET upozorňoval na potenciální riziko, klikněte na **Zobrazit možnosti** a zaškrtněte možnost **Vyloučit z detekce**.

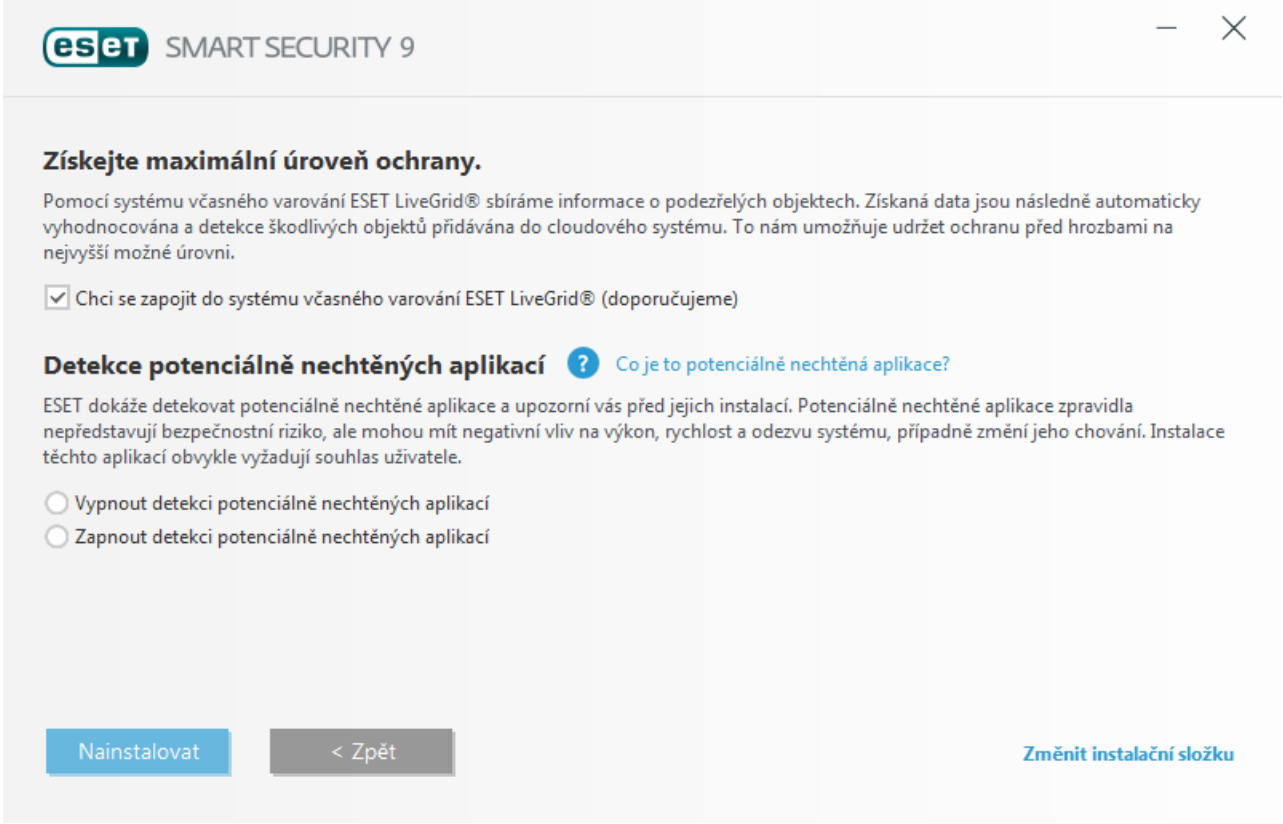


Pokud bude detekována potenciálně nechtěná aplikace a není možné ji vyléčit, při komunikaci dané aplikace se vzdálenou stranou se zobrazí upozornění **Adresa byla zablokována**. Zároveň se tato informace zapíše do protokolu a více informací naleznete v hlavním menu programu na záložce **Nástroje** > **Další nástroje** > **Protokoly** > **Filtrované webové stránky**.



Potenciálně nechtěné aplikace – Nastavení

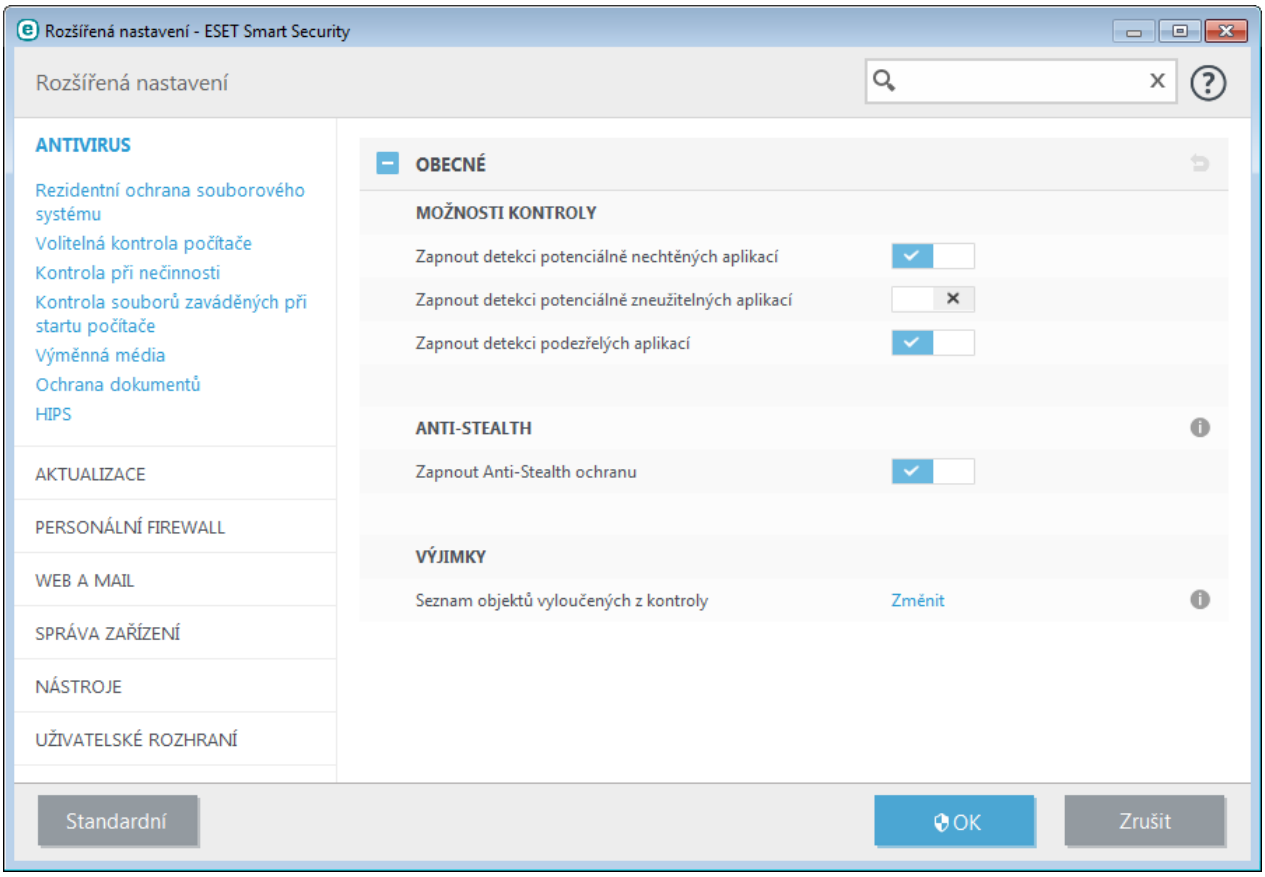
Již při instalaci produktu ESET se můžete rozhodnout, zda chcete být upozorňováni na potenciálně nechtěné aplikace:



Potenciálně nechtěné aplikace mohou do vašeho systému doinstalovat adware, toolbary nebo další aplikace, které mohou ve vašem systému provádět nechtěné a nebezpečné operace.

Nastavení detekce těchto aplikací můžete kdykoli změnit v nastavení programu. Pro úpravu detekce postupujte podle následujících kroků:

1. Otevřete hlavní okno produktu ESET. Pokud nevíte jak, postupujte podle tohoto návodu.
2. Stiskněte klávesu F5 a zobrazte **Rozšířená nastavení**.
3. Přejděte na záložku **Antivirus**, kde jsou dostupné následující možnosti: **Zapnout detekci potenciálně nechtěných aplikací**, **Zapnout detekci potenciálně zneužitelných aplikací** a **Zapnout detekci podezřelých aplikací**. Pro uložení změn klikněte na tlačítko **OK**.



Potenciálně nechtěné aplikace – Software wrappery

Software wrapper představuje speciální typ úpravy aplikace, který používají některé softwarové portály. Vámi požadovanou aplikaci nestahujete napřímo, ale prostřednictvím nástroje třetí strany. Tyto nástroje kromě požadované aplikace do systému instalují adware nebo toolbary. Kromě originální aplikace se mohou tyto nástroje, které dále mohou měnit domovskou stránku ve vašem prohlížeči a ovlivňovat výsledky vyhledávání. Protože softwarové portály v drtivé většině neinformují koncového uživatele, že ke stažení aplikace dojde prostřednictvím nástroje třetí strany, společnost ESET detekuje tzv. software wrappery jako potenciálně nechtěné aplikace. V takovém případě máte na výběr, zda chcete pokračovat ve stahování nebo si najít jiný zdroj.

Nejnovější verzi této kapitoly naleznete v ESET Databázi znalostí.

6.1.10 Botnet

Robot nebo webový robot je automatizovaný škodlivý kód, který skenuje síť a hledá zranitelné počítače. Tento způsob umožňuje tvůrcům škodlivého kódu ovládnout velké množství počítačů a proměnit je v tzv. zombie. Síť velkého množství takto ovládaných počítačů se nazývá botnet. Každý počítač zapojený do botnetu může útočníkovi sloužit jako zdroj DDoS útoků, proxy nebo pro provádění jiných automatizovaných síťových úloh (například odesílání spamu, krádeži citlivých dat jako jsou čísla bankovních účtů nebo kreditních karet), aniž by o tom uživatel daného počítače věděl.

6.2 Typy útoků

Existují různé techniky umožňující útočníkům napadnout vzdálené počítače. Podle povahy se útoky dělí do několika skupin.

6.2.1 DoS útoky

DoS neboli *Denial of Service* – odmítnutí služby, je způsob útoku, který způsobí, že prostředky počítače nebudou dostupné pro původní uživatele. Komunikace mezi uživateli je přetížená, neprobíhá správně a pro obnovení funkčnosti je nutné počítač restartovat.

Cílem se stávají nejčastěji webové servery, kdy účelem útoku je vyřadit je z provozu.

6.2.2 DNS Poisoning

DNS Poisoning („otrávení" pomocí odpovědi serveru DNS) je metoda, která dokáže oklamat počítač tím, že mu útočník podsune klamné informace o DNS serveru, které považuje za autentické. Nepravdivé informace počítač určitou dobu uchovává v mezipaměti, což útočníkovi umožňuje manipulaci s DNS odpověďmi z konkrétní IP adresy. Tím dokáže u uživatele vyvolat dojem, že navštěvuje legitimní internetovou stránku, ve skutečnosti mu však může být podsunut škodlivý obsah nebo se tímto způsobem do počítače stáhne počítačový vir nebo červ.

6.2.3 Útoky počítačových červů

Počítačový červ je program obsahující škodlivý kód, který napadá hostitelské počítače a šíří se dál prostřednictvím sítě. Tzv. síťoví červi zneužívají různé bezpečnostní chyby v mnoha aplikacích. Díky značnému rozšíření internetu se červ dokáže dostat do celého světa během několika hodin od vydání, v některých případech dokonce během několika minut.

Nejrozšířenější typy útoků (Sasser, SqlSlammer) je možné blokovat pomocí standardních nastavení firewallu, případně blokováním nepoužívaných portů nebo zabezpečením používaných portů. Důležitá je také instalace bezpečnostních záplat pro operační systém a další software.

6.2.4 Skenování portů

Port scanning (skenování portů) je činnost, která ověřuje, zda jsou v počítači otevřené porty. Skener portů je speciální software, který dokáže v síti zjistit případné otevřené porty.

Počítačový port si lze představit jako virtuální bod, kterým procházejí informace z a do počítače, takže z hlediska bezpečnosti jde o kritickou záležitost. Ve velkých sítích má tato činnost svoje opodstatnění, protože se jedná o rychlý způsob pro odhalení případných bezpečnostních rizik.

Právě proto patří skenování portů mezi často používanou techniku vzdálenými útočníky. Prvním krokem je zaslání paketů na každý port. Na základě odpovědi lze zjistit, zda se port používá. Pouhá kontrola sama o sobě ještě nezpůsobuje žádné škody, ale tato technika však umožňuje odhalit nedostatečně zabezpečený bod a získat kontrolu nad vzdáleným počítačem.

Správce sítě by tedy měl automaticky zablokovat nevyužívané porty a používané porty zabezpečit.

6.2.5 TCP desynchronizace

Desynchronizace protokolu TCP je technika využívaná při tzv. útocích TCP Hijacking. Desynchronizace je vyvolána procesem, kdy se sekvenční číslo přijatého paketu neshoduje s očekávaným sekvenčním číslem. V závislosti na sekvenčním čísle poté dojde k zahození paketu (případně k jeho uložení do vyrovnávací paměti, pokud se nachází v aktuálním okně komunikace).

Ve stavu desynchronizace si obě strany v komunikaci navzájem zahazují pakety. Do toho může vstoupit útočník (sledující danou komunikaci) a dodat pakety se správným sekvenčním číslem. Útočník může v takovém případě přidávat do komunikace příkazy nebo ji jinak pozměnit.

Cílem útoku je narušit spojení na úrovni klient-server, nebo P2P komunikaci. Zabránit takovému útoku je možné použitím autentifikace jednotlivých segmentů protokolu TCP nebo dodržováním doporučených nastavení pro správu a nastavení síťových zařízení.

6.2.6 SMB Relay

SMBRelay a SMBRelay2 jsou speciální programy, které dokáží provést útok na vzdálený počítač. Program využívá protokol pro sdílení souborů SMB (Server Message Block) provázaný s rozhraním NetBIOS. Pokud sdílíte složku nebo disk v rámci lokální sítě, využíváte s nejvyšší pravděpodobností tento způsob sdílení.

V rámci komunikace uvnitř lokální sítě poté dochází k výměně kontrolních součtů (hash) uživatelských hesel.

Program SMBRelay zachytává komunikaci na portu UDP 139 a 445, přesměruje pakety mezi klientem a serverem příslušné stanice a upraví je. Po připojení a autentifikaci je klientská stanice odpojena a program SMBRelay vytvoří novou virtuální IP adresu. K této adrese se poté lze připojit příkazem „net use \\192.168.1.1“ a adresa může být používána všemi integrovanými síťovými funkcemi systému Windows. Program přenáší veškerou komunikaci SMB kromě vyjednávání (negotiation) a autentifikace. Pokud je klientský počítač připojen, vzdálený útočník se může kdykoli připojit na uvedenou IP adresu.

Program SMBRelay2 pracuje na stejném principu, místo IP adres však používá názvy z rozhraní NetBIOS. Oba programy umožňují útoky typu „man-the-middle“ (člověk uprostřed), tedy útoky, kde útočník dokáže číst, zadávat a měnit odkazy mezi dvěma stranami bez toho, aby o tom některá ze stran věděla. Nejčastějším příznakem je, že systém přestane reagovat, nebo dojde k náhlému restartování počítače.

Doporučenou ochranou proti těmto útokům je používání autentifikace za pomoci hesel nebo klíčů.

6.2.7 Útoky prostřednictvím protokolu ICMP

Protokol ICMP (Internet Control Message Protocol) je jedním z hlavních internetových protokolů. Slouží k odesílání různých chybových hlášení a využívají ho k tomuto účelu zejména počítače a další zařízení v síti.

Útoky vedené protokolem ICMP zneužívají jeho slabá místa. ICMP je navržen pro jednosměrnou komunikaci bez ověřování. Tento fakt dovoluje vzdálenému útočníkovi vyvolat například tzv. DoS útok (Denial of Service) nebo útoky, které umožní sledování a přístup k paketům celé komunikace.

Typickými příklady ICMP útoků jsou ping flood, ICMP_ECHO flood nebo smurf attack. Mezi příznaky patří značné zpomalení internetových aplikací případně další problémy s připojením k internetu.

6.3 ESET Technologie

6.3.1 Exploit Blocker

Exploit Blocker představuje další bezpečnostní vrstvu, které chrání aplikace se zranitelnými bezpečnostními dírami (například webové prohlížeče, e-mailové klienty, pdf čtečky). Neustále shromažďuje informace o určitých procesech a na základě systémových akcí provádí kontrolu, zda nebyla bezpečnostní díra zneužita.

Při detekci zneužití bezpečnostní díry dojde okamžitě k zablokování běhu daného procesu a získaná data o hrozbě jsou odeslána do cloudového systému ThreatSense. Tato data budou následně analyzována ve virových laboratořích ESET a pomohou ochránit uživatele před neznámými novými a tzv. zero-day útoky (škodlivým kódem zneužívajícím dosud nezáplatované bezpečnostní díry).

6.3.2 Advanced Memory Scanner

Pokročilá kontrola paměti v kombinaci s funkcí Exploit Blocker poskytuje účinnou ochranu proti škodlivému kódu, který využívá obfuskaci a šifrování pro zabránění detekce. V případech, kdy emulace kódu nebo heuristika neodhalí hrozbu, pokročilá kontrola paměti dokáže identifikovat podezřelé chování škodlivý kód přímo v operační paměti. Toto řešení tak představuje efektivní ochranu před malware, který používá obfuskaci kódu.

Podobně jako Exploit Blocker také Pokročilá kontrola paměti analyzuje kód až po spuštění. Existuje tedy vždy riziko, že předtím než dojde k detekci hrozby, může škodlivý kód v systému provést nežádoucí aktivity. Přesto se jedná o další bezpečnostní vrstvu, která zastaví novou infiltraci, pokud všechny ostatní technicky detekce selhaly.

6.3.3 Štít zranitelností

Štít zranitelností je rozšíření Personální firewallu, které přináší vylepšenou detekci známých síťových typů útoků a zranitelností. Implementace detekce známých zranitelností v nejčastěji používaných síťových protokolech jako je SMB, RPC a RDP představuje další bezpečnostní vrstvu, která zajišťuje ochranu proti širokému spektru škodlivých kódů, síťových útoků a zranitelností v síťových protokolech, které dosud nebyly opraveny.

6.3.4 ThreatSense

Vestavěný systém včasného varování ThreatSense.Net® sbírá anonymní data od uživatelů ESET a odesílá vzorky do virových laboratoří ESET. Poskytnutím vzorku infiltrace a dalších dat do systému ThreatSense umožňuje společnosti ESET okamžitě reagovat na výskyt nových hrozeb a chránit tak své zákazníky. Specialisté ve virových laboratořích ESET tyto informace používají pro sestavení přesného obrazu o povaze a rozsahu hrozby, což nám umožňuje připravit vhodné řešení. Data odeslaná do ThreatSense představují důležitou roli při určování priorit během automatického zpracovávání.

Dále obsahuje systém reputace, který zlepšuje celkovou efektivitu našeho anti-malware řešení. Každý spuštěný soubor nebo otevřený archiv je analyzován a opatřen unikátním identifikátorem, pomocí kterého je následně porovnáván vůči databázi povolených a blokovaných položek. Pokud je soubor nalezne na seznamu povolených, bude označen jako čistý a do budoucna bude vyloučen z kontroly. Pokud se nachází na seznamu blokovaných, provede se akce v závislosti na povaze hrozby. V případě, že nebude nalezena shoda v databázi, soubor bude zkontrolován. Následně na základě výsledku kontroly dojde k označení souboru podle toho, zda je čistý nebo infikovaný. To ve výsledku vede k nižšímu zatížení systému během kontroly počítače a zkrácení potřebné doby na kontrolu počítače.

Tento systém reputace poskytuje účinný způsob detekce škodlivého kódu ještě předtím, než jeho přesný vzorek bude zahrnut v další aktualizaci virové databáze.

6.3.5 Ochrana před zapojením do botnetu

Ochrana před zapojením do botnetu analyzuje síťovou komunikaci a protokoly, které využívá škodlivý kód při komunikaci s botnetem, a díky tomu odhalí a odstraní škodlivý kód, který se snaží váš počítač zapojit do botnetu.

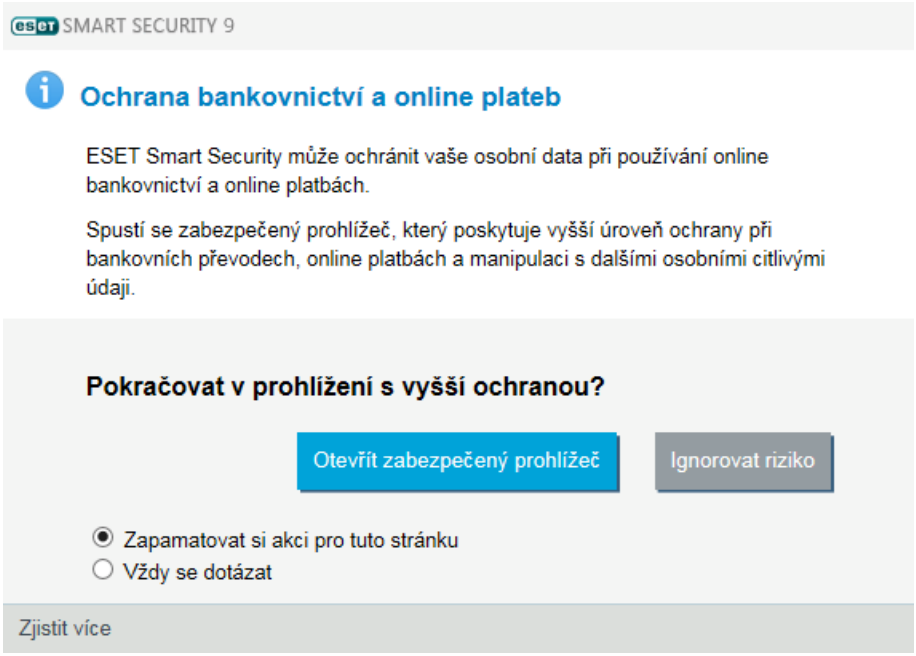
6.3.6 Java Exploit Blocker

Java Exploit Blocker rozšiřuje stávající ochranu Exploit Blocker a zabraňuje zneužití bezpečnostních děr v doplňku Java. Zablokované vzorky jsou následně automaticky odeslány k analýze do virové laboratoře ESET pro přidání obrany před tímto vzorkem do další aktualizace virové databáze.

6.3.7 Ochrana bankovnictví a online plateb

Ochrana bankovnictví a online plateb přidává další ochrannou vrstvu do internetového prohlížeče. Tato vrstva se stará o to, aby vaše osobní data (čísla bankovních účtů, kreditních karet atp.) nebyla v průběhu online transakcí zneužita, resp. nemohly je získat jiné aplikace. ESET Smart Security obsahuje vestavěný předdefinovaný seznam známých stránek internetového bankovnictví. Při přístupu na stránku z tohoto seznamu se vás ESET Smart Security zeptá, zda chcete danou stránku otevřít v zabezpečeném prohlížeči. Tento seznam můžete kdykoli rozšířit o internetový portál vaší banky.

Ochrana bankovnictví se spustí automaticky při přístupu na stránky internetového bankovnictví.



Následně klikněte na tlačítko **Otevřít zabezpečený prohlížeč**. Pokud ponecháte vybranou možnost **Zapamatovat si akci pro tuto stránku**, při dalším přístupu na stejnou webovou stránku se automaticky zobrazí v zabezpečeném prohlížeči. Své rozhodnutí můžete kdykoli změnit v Rozšířeném nastavení (dostupném po stisknutí **klávesy F5** v hlavním okně programu) na záložce **Web a mail** > **Ochrana bankovnictví a online plateb**.

Poznámka: Zabezpečený prohlížeč můžete kdykoli spustit ručně prostřednictvím ikony na Ploše nebo v hlavním menu ESET Smart Security přejděte na záložku Nástroje a vyberte možnost Ochrana bankovnictvím a online plateb. Zabezpečený prohlížeč nedoporučujeme používat pro běžné surfování na internetu a po ukončení online transakce jej ukončete.

Předpokladem pro fungování této vrstvy je HTTPS šifrovaná komunikace. To znamená, že stránky internetového bankovnictví vaší banky musí běžet na HTTPS. Abyste mohli využít této funkce, musíte používat některý z podporovaných internetových prohlížečů:

- Mozilla Firefox 24 a novější,
- Internet Explorer 8 a novější,
- Google Chrome 30 a novější.

Více informací o ochraně bankovnictví a online plateb naleznete v ESET Databázi znalostí:

- Jak používat ochranu bankovnictví a online plateb?
- Jak vypnout ochranu bankovnictví a online plateb?

6.4 Elektronická pošta

Elektronická pošta, tedy e-mail přináší jako moderní forma komunikace spoustu výhod. Je flexibilní, rychlá a přímá, a byla vlastně hlavním důvodem, proč se internet v první polovině devadesátých let minulého století rozšířil po celém světě.

Bohužel díky vysoké míře anonymity vznikl prostor pro zneužívání internetu a elektronické pošty k nelegálním účelům a šíření nevyžádané pošty. Nevyžádaná pošta je poměrně širokou kategorií zahrnující například reklamy, fámy a šíření škodlivého software (malware). Nebezpečí umocňuje fakt, že náklady na rozesílání jsou v podstatě nulové a tvůrci mají k dispozici spoustu nástrojů a zdrojů na zjištění nových e-mailových adres. Množství nevyžádané pošty se tím stává těžko regulovatelné a běžný uživatel elektronické pošty je v podstatě neustále vystavován nebezpečným útokům. Čím déle je e-mailová schránka používána, tím se zvyšuje pravděpodobnost, že se dostane do databáze tvůrců nevyžádané pošty. Několik tipů na prevenci:

- pokud je to možné, nezveřejňujte svou e-mailovou adresu na internetu,
- poskytujte svoji e-mailovou adresu co nejméně,
- používejte ne zcela běžné aliasy – složitější aliasy jsou obtížněji zjistitelné technikami používanými při rozesílání nevyžádané pošty,
- neodpovídejte na nevyžádanou poštu, kterou jste obdrželi,
- věnujte pozornost vyplňování formulářů na internetu – zejména automaticky zaškrtnutým možnostem typu "Ano, chci dostávat do své schránky informace o novinkách",
- používejte více "specializovaných" e-mailových adres – např. pracovní e-mail, e-mail pro komunikaci s přáteli a další,
- jednou za čas změňte e-mailovou adresu,
- používejte antispamové řešení.

6.4.1 Reklamy

Reklama na internetu patří mezi nejrychleji rostoucí formy reklamy. Nabídky zasílané prostřednictvím e-mailu jsou jednou z forem internetové reklamy. Jejich hlavní výhodou jsou téměř nulové náklady, přímé a okamžité doručení adresátovi. Mnoho společností se snaží tímto způsobem udržovat kontakt se svými stávajícími zákazníky, případně získávat nové, protože se jedná o účinný marketingový nástroj.

Reklama zasílaná e-mailem je sama o sobě legitimní. Uživatel může mít zájem získávat reklamní informace z určité oblasti. Často si však nepřeje, aby mu reklama byla zasílána, ale přesto se tak děje. V takovém případě se reklamní e-mail stává zároveň nevyžádanou poštou – spamem.

V současné době se množství nevyžádaných reklamních e-mailů stalo velkým problémem. Tvůrci nevyžádané pošty se přirozeně snaží spam maskovat jako legitimní zprávu.

6.4.2 Fámy

Fáma (z anglického "hoax") je internetem masově šířena zpráva. Nejčastějším médiem je elektronická pošta, případně komunikační nástroje typu ICQ a Skype. Jedná se buď o falešnou poplašnou zprávu, žert, nebo mystifikaci – zpráva sama o sobě se nezakládá na pravdě.

Mezi často rozšířené fámy patří například informace o novém počítačovém viru, který má běžné (vymazání souborů, získávání hesel), nebo až přímo absurdně znějící schopnosti a snaží se vyvolat v uživateli strach.

U některých poplašných zpráv se snaží autoři zajistit co největší rozšíření zprávy výzvami na další přeposlání pod různými záminkami. Časté jsou fámy o mobilních telefonech, prosby o pomoc, nabídky na velké částky peněz ze zahraničí. Ve většině případů je obtížné zjistit původní záměr autora.

V zásadě platí pravidlo, že pokud zpráva obsahuje výzvu k dalšímu hromadnému rozesílání, jedná se s největší pravděpodobností o hoax. Na internetu existuje několik specializovaných stránek s databází fám (hoaxů), na kterých si ověřte pravost takové zprávy předtím, než ji přepošlete dále.

6.4.3 Phishing

Pojem phishing definuje kriminální činnost využívající tzv. sociální inženýrství (technika manipulace s uživateli vedoucí k získávání důvěrných informací). Cílem je získat citlivé údaje, jako například hesla k bankovním účtům, PIN kódy a jiné detaily.

Phishingem označujeme falešný e-mail tvářící se důvěryhodně, který se snaží vzbudit dojem, že jeho odesílatelem je například banka nebo pojišťovna. Grafický vzhled zprávy, nebo stránka, na kterou zpráva odkazuje, je na první pohled nerozeznatelná od té, kterou instituce používá. Pod různými záminkami, například ověření přístupových údajů, zaslání částky peněz na účet atd. jsou od uživatelů získány důvěrné informace. Ty mohou být později zneužity v neprospěch poškozeného.

Nejlepší obranou proti phishingu je na takové zprávy vůbec neodpovídat. Banky a další instituce od vás prostřednictvím e-mailu nebudou nikdy vyžadovat uživatelské jméno a heslo.

6.4.4 Rozpoznání nevyžádané pošty

Existuje několik znaků, podle kterých se dá rozpoznat, zda je přijatá e-mailová zpráva nevyžádanou poštou. Pokud daná zpráva splňuje některou z následujících podmínek, jedná se pravděpodobně o nevyžádanou poštu – spam.

- Adresa odesílatele nepatří do vašeho seznamu kontaktů.
- Dostanete výhodnou finanční nabídku, ale žádá se od vás vstupní poplatek.
- Pod různými záminkami (ověření údajů, přesun financí) jsou od vás požadovány citlivé přístupové údaje (např. číslo bankovního účtu, heslo do internetového bankovnictví apod.).
- Zpráva je napsána v cizím jazyce.
- Zpráva nabízí produkt, o který se nezajímáte. Pokud máte přece jen o produkt zájem, je vhodné si ověřit přímo u výrobce, zda odesílatel zprávy patří mezi důvěryhodné distributory.
- Zpráva obsahuje zkomolená slova, aby oklamala filtry pro nevyžádanou poštu. Například místo "viagra" ve zprávě bude "vaigra " a podobně.

6.4.4.1 Pravidla

Pravidlo v antispamovém programu, případně poštovním klientu je účinným nástrojem pro správu pošty. Pravidlo se skládá ze dvou logických částí:

1) Podmínka (například příchod zprávy z určité adresy),

2) Akce (například vymazání zprávy nebo přesunutí do předem určené složky).

Množství a variabilita pravidel závisí na použitém antispamovém modulu. Jejich funkcí je třídění pošty do logických celků a její správa. Mohou zároveň sloužit i jako opatření proti nevyžádané poště. Typické příklady:

- 1. Podmínka: Přijde zpráva obsahující slovo typické pro nevyžádanou poštu.
  2. Akce: Vymazat zprávu.
- 1. Podmínka: Příchozí zpráva obsahuje jako přílohu soubor s příponou .exe.
  2. Akce: Vymazat přílohu a zprávu uložit do schránky.
- 1. Podmínka: Přijde zpráva z domény zaměstnavatele.
  2. Akce: Zařadit zprávu do záložky "Pracovní."

Doporučujeme používat kombinace několika pravidel pro zajištění efektivního filtrování nevyžádané pošty.

6.4.4.2 Seznam důvěryhodných adres (Whitelist)

Whitelist (v překladu "bílý seznam") je obecně seznam položek, případně osob, které jsou akceptovány, nebo mají někam zajištěn přístup. Pojmem e-mailový whitelist se označuje seznam kontaktů, od kterých chcete přijímat e-maily. Seznamy můžete vytvářet na základě klíčových slov, které jsou pak vyhledávány v e-mailových adresách, názvů domén nebo IP adres.

Pokud je whitelist nastaven do režimu výjimek, zprávy z jiných adres, domén nebo IP adres se do pošty nedostanou. Pokud se whitelist sice používá, ovšem ne v režimu výjimek, nevyžádaná pošta se přesune do schránky s nevyžádanou poštou.

Whitelist je založen na opačném principu než blacklist. Výhodou whitelistu je, že není tak náročný na údržbu jako blacklist. Obě metody můžete vhodně zkombinovat a dosáhnout tak účinného filtrování nevyžádané pošty.

6.4.4.3 Seznam spamových adres (Blacklist)

Blacklist (v překladu "černý seznam") je obecně seznam zakázaných položek/osob a ve virtuálním světě představuje mechanismus, který povoluje přijímání elektronické pošty od všech odesílatelů, kteří se na blacklistu nenacházejí.

Existují dva druhy blacklistu. Uživatelsky definovaný seznam přímo v antispamovém řešení nebo veřejné dostupný pravidelně aktualizovaný blacklist vydávaný renomovanými institucemi.

Jeho používání má velký význam pro blokování elektronické pošty. Je však náročný na údržbu, protože nové adresy, které je potřeba přidat do seznamu, se objevují neustále. Vhodnou kombinací whitelistu a blacklistu můžete docílit efektivního filtrování nevyžádané pošty.

6.4.4.4 Seznam výjimek

Na seznam výjimek se zpravidla přidávají e-mailové adresy, které byly zneužity a jsou využívány pro rozesílání nevyžádané pošty. Zprávy rozesílané z adres uvedených na tomto seznamu tak budou vždy kontrolovány na přítomnost spamu. ESET Smart Security na tento seznam automaticky přidá všechny e-mailové adresy z poštovních účtů definovaných v poštovních klientech. V případě potřeby můžete tento seznam kdykoli rozšířit.

6.4.4.5 Kontrola na serveru

Kontrola na serveru je technika pro odhalování hromadných nevyžádaných zpráv na základě jejich počtu a uživatelské reakce. Na základě obsahu hlavní části zprávy se vypočítá digitální otisk. Unikátní ID číselná hodnota zprávy neposkytuje žádnou informaci o obsahu zprávy, kromě toho, že dvě stejné zprávy budou mít stejný otisk, zatímco dvě různé zprávy budou mít téměř jistě otisk různý.

Pokud uživatel označí danou zprávu jako nevyžádanou poštu, odešle se na server její otisk. Pokud server obdrží více identických otisků, uloží jej do své databáze otisků nevyžádané pošty. Při kontrole došlé pošty znovu program odesílá na server otisky přijatých zpráv. Server následně vrátí informaci, které zprávy označili ostatní uživatelé jako nevyžádané.

7. Řešení nejčastějších problémů

Tato kapitola obsahuje některé z nejčastěji se vyskytujících otázek a problémů, se kterými se můžete setkat. Klikněte na název kapitoly pro zobrazení řešení problému.

Jak aktualizovat ESET Smart Security?
Jak aktivovat ESET Smart Security?
Jak odstranit vir z počítače?
Jak povolit komunikaci pro konkrétní aplikaci?
Jak vytvořit novou úlohu v Plánovači?
Jak naplánovat kontrolu počítače (kontrola každých 24 hodin)?

Pokud není váš problém zahrnut v seznamu výše, zkuste v nápovědě ESET Smart Security vyhledat řešení podle klíčového slova nebo fráze, která popisuje váš problém. Pokud nenaleznete řešení vašeho problému v nápovědě, navštivte pravidelně aktualizovanou ESET Databázi znalostí. Níže naleznete odkazy na nejnavštěvovanější články v databázi.

Při aktivaci produktu ESET došlo k chybě. Co to znamená?
Jak zadat Uživatelské jméno a Heslo do programu ESET Smart Security/ESET NOD32 Antivirus?
Instalace programu ESET skončila předčasně
Co musím udělat po obnovení licence? (Domácí uživatelé)
Co se stane, pokud změním e-mailovou adresu?
Jak spustit Windows v Nouzovém režimu nebo Nouzovém režimu se sítí

Pokud je to nutné, můžete se obrátit přímo na naše pracovníky technické podpory. Kontaktní formulář naleznete přímo v programu na záložce **Nápověda a podpora**.

7.1 Jak aktualizovat ESET Smart Security?

Aktualizaci ESET Smart Security můžete provádět ručně nebo automaticky. Pro zahájení aktualizace klikněte na tlačítko **Aktualizovat** na záložce **Aktualizace**.

Po nainstalování programu se standardně vytvoří naplánovaná úloha, která spouští automatickou aktualizaci každou hodinu. Pokud chcete změnit tento interval, přejděte na záložku **Nástroje** > **Plánovač** (pro více informací týkajících se Plánovače klikněte sem).

7.2 Jak odstranit vir z počítače?

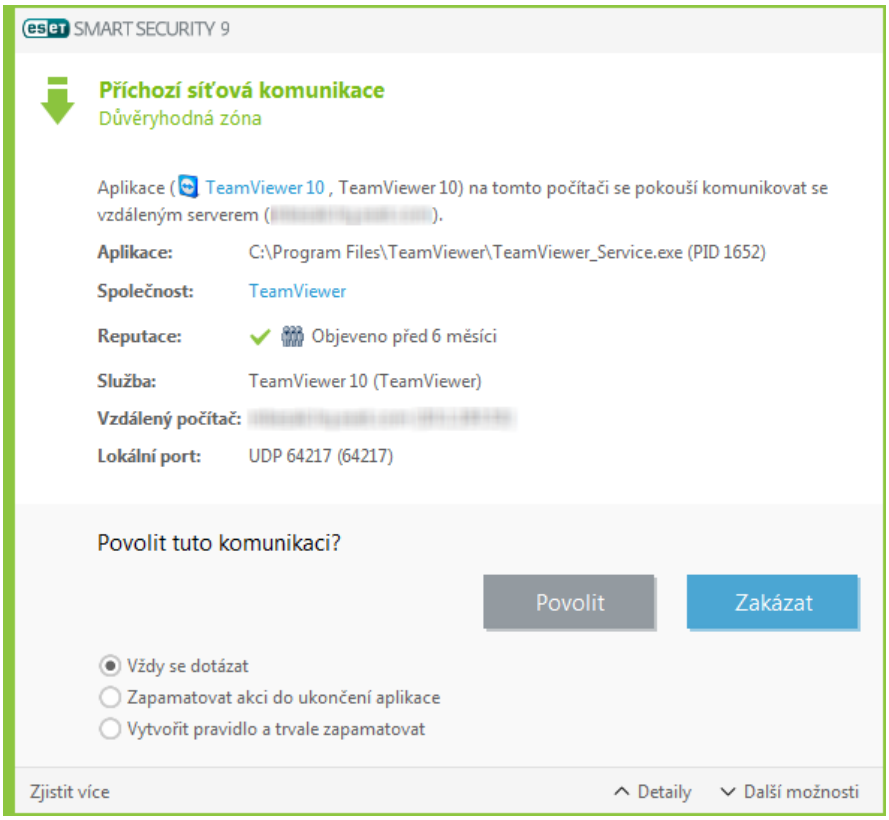
Pokud jeví počítač známky infekce, tzn. je pomalejší, zamrzá apod. doporučujeme postupovat podle následujících kroků:

1. V hlavním okně programu klikněte na záložku **Kontrola počítače**,
2. Klikněte na možnost **Smart kontrola** pro zahájení kontroly počítače,
3. Po ukončení kontroly prověřte protokol zkontrolovaných, infikovaných a vyléčených souborů,
4. Pokud chcete zkontrolovat pouze určité části počítače, vyberte možnost **Volitelná kontrola** a ručně vyberte cíle kontroly.

Pro více informací přejděte do Databáze znalostí.

7.3 Jak povolit komunikaci pro určitou aplikaci?

Pokud je detekováno nové spojení/komunikace v interaktivním režimu Personálního firewallu, pro kterou ještě nebylo vytvořeno pravidlo, zobrazí se dialogové okno, ve kterém můžete komunikaci povolit nebo zakázat. Pokud chcete, aby se ESET Smart Security provedl vybranou akci při každém pokusu o komunikaci, zaškrtněte možnost **Zapamatovat akci (vytvořit pravidlo)**.



Pro aplikace, které dosud ESET Smart Security Personální firewall nedetekoval můžete vytvořit nové pravidlo v Rozšířeném nastavení (dostupném po stisknutí klávesy F5 v hlavním okně programu) ve větvi **Síť** > **Personální firewall** > **Pravidla a zóny** > **Nastavení**. V okně **Pravidla a zóny** se přepněte na záložku **Pravidla**. Je nutné mít Personální firewall přepnut v Interaktivního režimu.

Na záložce **Všeobecné** zadejte název pravidla, směr a komunikační protokol pro nové pravidlo. V tomto okně můžete definovat akci, která se provede při aplikaci daného pravidla.

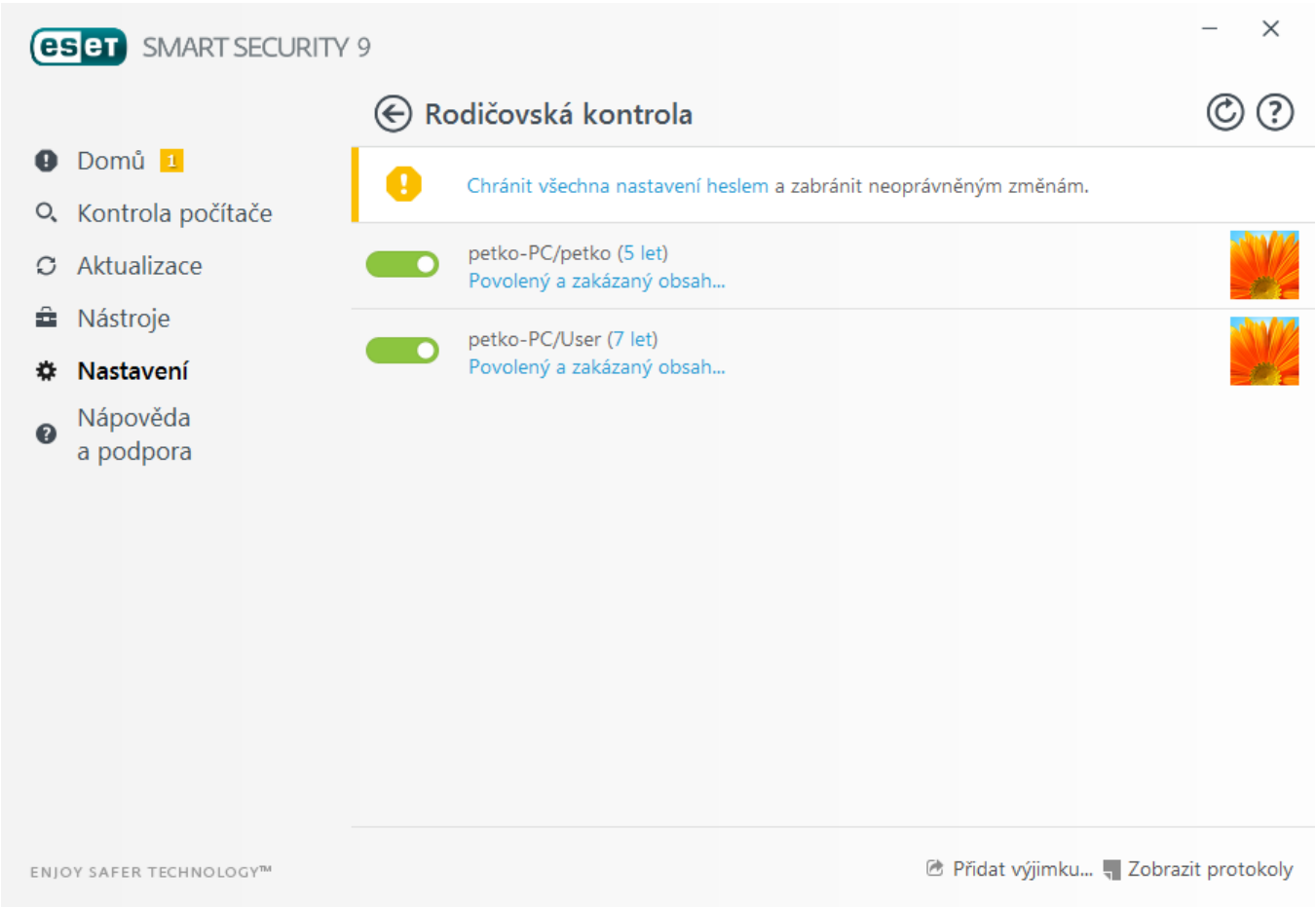
Zadejte cestu ke spustitelné aplikaci (*.exe) a lokální port na záložce **Lokální strana**. Přejdete na záložku **Vzdálená strana**, kde zadejte **Vzdálenou adresu** a **Port** (pokud je to potřeba). Nově vytvořené pravidlo se aplikuje ihned po detekci dané komunikace.

7.4 Jak aktivovat rodičovskou kontrolu?

Pro aktivování Rodičovské kontroly pro vybraný uživatelský účet postupujte podle následujících kroků.

1. V základním nastavení je Rodičovská kontrola vypnuta. Zapnout ji můžete dvěma způsoby:
   - Pomocí přepínače na záložce **Nastavení** > **Bezpečnostní nástroje** aktivujte rodičovskou kontrolu.
   - V hlavním okně programu stiskněte **klávesu F5** pro zobrazení Rozšířeného nastavení. V levé části klikněte na **Web a mail** > **Rodičovská kontrola** a v pravé části zaškrtněte možnost **Zapnout rodičovskou kontrolu**.
2. Klikněte na záložku **Nastavení** > **Bezpečnostní nástroje** > **Rodičovská kontrola** v hlavním okně programu. Přesto, že je funkce aktivována, musíte definovat uživatelské účty, pro které se má použít. To provedete kliknutím na možnost **Ochránit tento účet**. V nastavení účtu vyberte věk, který odpovídá danému uživateli, podle něhož se stanovuje úroveň filtrování webových stránek. Nyní bude Rodičovská kontrola aktivní pro vybraný uživatelský účet. Dále klikněte na možnost **Povolený a zakázaný obsah...** a přejděte na záložku Filtrování obsahu webu pro

přizpůsobení kategorií stránek, které chcete povolit nebo blokovat. Pro blokování konkrétních stránek přejděte na záložku Blokované a povolené webové stránky.



7.5 Jak vytvořit novou úlohu v Plánovači?

Pro vytvoření nové úlohy v Plánovači přejděte v hlavním okně programu na záložku **Nástroje** > **Plánovač** a klikněte na tlačítko **Přidat** v dolní části okna nebo z kontextového menu dostupného po kliknutím pravým tlačítkem myši. K dispozici jsou následující typy úloh:

- **Spuštění externí aplikace** – poskytne výběr aplikace, kterou má plánovač spustit,
- **Údržba protokolů** – defragmentace odstraní prázdné záznamy v protokolech. Viditelné zlepšení práce s protokoly po optimalizaci je především při větším množství záznamů v protokolech,
- **Kontrola souborů spouštěných při startu** – kontroluje soubory, které se spouštějí při startu nebo po přihlášení do systému,
- **Vytvoření záznamu o stavu počítače** – vytvoří záznam systému pomocí ESET SysInspector, který slouží k důkladné kontrole stavu počítače a umožňuje zobrazit získané údaje v jednoduché a čitelné formě,
- **Volitelná kontrola počítače** – provede volitelnou kontrolu disků, jednotlivých složek a souborů na počítači,
- **Prvotní kontrola** – standardně se spustí po 20 minutách od instalace produktu nebo restartování počítače.
- **Aktualizace** – zajišťuje aktualizaci virových databází i aktualizaci všech programových komponent systému.

Mezi nejčastěji používané naplánované úlohy patří **Aktualizace**, proto si podrobněji popíšeme přidání nové aktualizační úlohy.

Po zobrazení nabídky naplánovaných úloh vyberte z rozbalovacího menu položku **Aktualizace**. Zadejte název úlohy. a klikněte na tlačítko **Další**. Dále nastavte pravidelnost opakování úlohy. K dispozici jsou možnosti: **Jednou**, **Opakovaně**, **Denně, Týdně**, **Při události**. Možnost **Nespouštět úlohu, pokud je počítač napájen z baterie** je dobré použít, pokud přenosný počítač není zapojen do elektrické sítě a chcete v tomto čase minimalizovat jeho systémové prostředky. Dále je potřeba definovat akci, která se provede v případě, že ve stanoveném termínu nebude možné úlohu spustit. K dispozici jsou následující možnosti:

- **Při dalším naplánovaném termínu**
- **Jakmile to bude možné**
- **Okamžitě, pokud od posledního provedení uplynul stanovený interval** (definovaný v poli **Čas od posledního spuštění**)

V dalším kroku se zobrazí souhrnné informace o přidávané naplánované úloze. Akci dokončete kliknutím na tlačítko **Dokončit.**

V zobrazeném dialogovém okně vybrat profil, který se použije pro aktualizaci. Vybrat můžete primární a alternativní profil, který se použije v případě, že úlohu nebude možné provést pomocí primárního profilu. Kliknutím na tlačítko **Dokončit** se vytvořená naplánovaná úloha přidá do seznamu naplánovaných úloh.

7.6 Jak naplánovat kontrolu počítače (kontrola každých 24 hodin)?

Pro naplánování standardní úlohy přejděte v hlavním okně programu na záložku **Nástroje** > **Plánovač**. Níže je popsán stručný návod, jak vytvořit úlohu, která bude kontrolovat lokální disky každých 24 hodin. Více informací naleznete v Databázi znalostí.

Pro naplánovaní úlohy postupujte následovně:

1. Klikněte na tlačítko **Přidat** v hlavním okně **Plánovače**,
2. V rozbalovacím menu vyberte možnost **Kontrola počítače**,
3. Zadejte název úlohy a klikněte na možnost **Opakovaně**,
4. Interval provedení úlohy zadejte 24 hodin (1440 minut),
5. Vyberte akci, která se provede v případě neprovedení úlohy ve stanoveném čase,
6. Zkontrolujte všechna nastavení úlohy v seznamu a klikněte na **Dokončit**,
7. V rozbalovacím menu **Cíle kontroly** vyberte lokální disky,
8. Klikněte na **Nastavit** pro dokončení.

7.7 Jak přeinstalovat ESET Smart Security?

Důležité: Mějte na paměti, že po odinstalování produktu ESET nebude váš počítač chráněn. Pokud budete přistupovat pouze na webové stránky společnosti ESET, nehrozí vám nebezpečí.

Pro přeinstalování produktu ESET Smart Security postupujte podle následujících kroků:

1. Klikněte na **Start** > **Ovládací panely** > **Programy a funkce** (Přidat nebo odebrat programy).
   Tip: Od Windows 7 v Nabídce Start můžete rovnou psát. Stačí tedy napsat prvních pár znaků ze slova **Programy a funkce**.
2. V seznamu aplikací najděte ESET Smart Security a klikněte na tlačítko **Změnit/Odinstalovat**. Postupujte podle kroků na obrazovce a po odinstalování produktu restartujte počítač
3. Proveďte novou instalaci.

Více informací naleznete v Databázi znalostí:

- Postup pro Windows 8
- Postup pro Windows 10

Pokud je instalace poškozená, bude nutné program odinstalovat v nouzovém režimu prostřednictvím nástroje ESET Uninstaller.